

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日                      2 0 0 3 年    3 月 1 9 日  
Date of Application:

出 願 番 号                      特 願 2 0 0 3 - 0 7 5 8 6 5  
Application Number:  
[ST. 10/C]:                      [ J P 2 0 0 3 - 0 7 5 8 6 5 ]

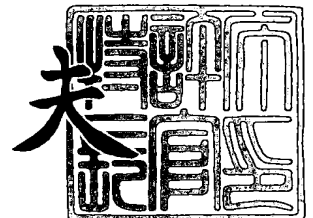
出      願      人                      株式会社日立製作所  
Applicant(s):

U.S. Appln. Filed 3-18-04  
Inventor: T. Yasue et al  
Manningly Stanger & Malor  
Docket HAS-101

2 0 0 4 年    3 月    4 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号    出証特 2 0 0 4 - 3 0 1 6 8 6 6

【書類名】 特許願

【整理番号】 P0637JP

【提出日】 平成15年 3月19日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/46

【発明者】

【住所又は居所】 神奈川県秦野市堀山下 1 番地 株式会社日立製作所 エ  
ンタープライズサーバ事業部内

【氏名】 安江 利一

【発明者】

【住所又は居所】 神奈川県秦野市堀山下 1 番地 株式会社日立製作所 エ  
ンタープライズサーバ事業部内

【氏名】 綿貫 達哉

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社日立製作所

【代理人】

【識別番号】 100107010

【弁理士】

【氏名又は名称】 橋爪 健

【手数料の表示】

【予納台帳番号】 054885

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0104115

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ネットワーク認証装置及びネットワーク認証システム

【特許請求の範囲】

【請求項 1】

ユーザ認証を行い、ネットワークを介してユーザ端末と情報サーバとの間でパケットを送受信するネットワークシステムにおけるネットワーク認証装置であって、

ユーザ端末及び情報サーバに対してパケットを送受信するネットワークインタフェース部と、

受信したパケットを中継すべき前記ネットワークインタフェース部を示す情報が登録されるアドレステーブルと、

入力されたパケットを、該パケットの宛先アドレスに基づき、前記アドレステーブルが示す前記ネットワークインタフェース部を介して中継するパケット中継部と、

パケットの中継又は廃棄を示す情報が登録されており、認証されたユーザ端末からのパケットを中継するように情報が更新されるフィルタリングテーブルを有し、前記ネットワークインタフェース部を介して受信したパケットの宛先アドレスに対応する、送信元MACアドレスと送信元IPv6アドレスとの両方の情報に基づき、前記フィルタリングテーブルを参照して条件を判断し、該受信したパケットを前記パケット中継部へ中継する又は廃棄するフィルタリング処理部と、を備えたネットワーク認証装置。

【請求項 2】

送信元IPv6アドレスとして、送信元IPv6アドレスのインタフェース識別子を用いる請求項 1 に記載のネットワーク認証装置。

【請求項 3】

ユーザ認証によりアクセスが許可されたユーザ端末からのパケットを中継させるための状態変更指示を受信し、該状態変更指示に従い前記フィルタリングテーブルを変更するフィルタ変更指示処理部をさらに備え、

前記フィルタリング処理部は、変更された前記フィルタリングテーブルに基づ

いて、アクセスが許可されたユーザ端末からのパケットを中継する請求項1に記載のネットワーク認証装置。

【請求項4】

前記フィルタリング処理部は、受信したパケットから宛先アドレス、送信元MACアドレス及び送信元IPv6アドレスの複数の情報を抽出し、前記フィルタリングテーブルの対応する情報と比較し、全ての情報で中継と判断した場合に該パケットを前記パケット中継部へ中継する請求項1に記載のネットワーク認証装置。

【請求項5】

前記フィルタリング処理部は、

宛先MACアドレス及び送信元MACアドレスに対応して受信パケットの中継又は廃棄を示す情報が登録されたMACアドレスフィルタリングテーブルと、

宛先IPv6アドレス及び送信元IPv6アドレスに対応して受信パケットの中継又は廃棄を示す情報が登録されたIPv6アドレスフィルタリングテーブルと、

前記MACアドレスフィルタリングテーブルを参照して、受信パケットを中継又は廃棄するMACアドレス処理部と、

前記IPv6アドレスフィルタリングテーブルを参照して、受信パケットを中継又は廃棄するIPv6アドレス処理部と  
を有し、

前記MACアドレス処理部と前記IPv6アドレス処理部との両方で中継すると判断された受信パケットのみ、前記パケット中継部へ中継する請求項1に記載のネットワーク認証装置。

【請求項6】

ユーザ識別子、パスワード、IPv6アドレスのインタフェース識別子及びMACアドレスが記憶され、ユーザ端末からの要求に従いユーザ認証を行う認証処理部をさらに備えた請求項1に記載のネットワーク認証装置。

【請求項7】

前記認証処理部は、

ユーザ端末からのユーザ認証要求を受け付け、ユーザ識別子、パスワード、MACアドレス、IPv6アドレス又は該アドレスのインタフェース識別子のいずれか又は複数を含む認証パラメータをユーザ端末から受け取る認証受付処理部と、

ユーザ端末から受け取った認証パラメータと予め記憶された認証用データとに基づきユーザ及びその端末を認証し、認証した場合に、前記フィルタ変更指示処理部に認証したユーザ端末からのパケットを中継させるための状態変更指示を送信する認証部

を有する請求項6に記載のネットワーク認証装置。

#### 【請求項8】

通信相手毎に鍵交換処理を行って通信パスを確立し、通信相手毎に鍵交換処理により作成した鍵、及び、通信相手の認証を行うための予め定められた鍵若しくは認証情報を格納するIPセキュリティ制御部と、

前記IPセキュリティ制御部により作成された鍵を用いたパケットの暗号化及び復号化機能、及び、パケット改ざんチェック機能、及び、前記IPセキュリティ制御部に記憶されている予め定められた鍵若しくは認証情報に基づく通信相手の認証機能とを有するIPセキュリティ処理部とをさらに備え、

前記IPセキュリティ処理部は、通信相手を認証した場合にパケットを前記フィルタリング処理部へ送信し、一方、認証されなかった場合にパケットを廃棄する請求項1に記載のネットワーク認証装置。

#### 【請求項9】

請求項1に記載のネットワーク認証装置と、

ネットワークを介して前記ネットワーク認証装置に接続されたユーザ端末と、前記ネットワーク認証装置に接続され、前記ユーザ端末に対してデータを提供する情報サーバと、

前記ネットワーク認証装置に接続され、前記ユーザ端末からの認証要求に従い、前記情報サーバへのアクセスを許可するための認証を行う認証サーバと、を備え、

前記認証サーバは、前記ユーザ端末から、ユーザ識別子、パスワード、MAC アドレス、IPv6 アドレス又は該アドレスのインタフェース識別子のいずれか又は複数を含む認証パラメータを受け取り、

該認証パラメータと予め記憶されている認証用データに基づき前記ユーザ端末を認証し、前記ネットワーク認証装置に、認証した前記ユーザ端末から前記情報サーバへの packets を中継させるネットワーク認証システム。

【請求項 10】

前記ネットワーク認証装置と前記ユーザ端末は、広域イーサネット（登録商標）網で接続されていることを特徴とする請求項 9 に記載のネットワーク認証システム。

【請求項 11】

請求項 1 に記載のネットワーク認証装置と、  
packets を中継するためのルータと、  
前記ルータ及びネットワークを介して前記ネットワーク認証装置に接続されたユーザ端末と、  
前記ネットワーク認証装置に接続され、前記ユーザ端末に対してデータを提供する情報サーバと、  
前記ルータに接続され、前記ユーザ端末からの認証要求に従い、前記情報サーバへのアクセスを許可するための認証を行う認証サーバと、  
を備え、

前記認証サーバは、前記ユーザ端末から、ユーザ識別子、パスワード、MAC アドレス、IPv6 アドレス又は該アドレスのインタフェース識別子のいずれか又は複数を含む認証パラメータを受け取り、

該認証パラメータと予め記憶されている認証用データに基づき前記ユーザ端末を認証し、前記ネットワーク認証装置に、認証した前記ユーザ端末から前記情報サーバへの packets を中継させるネットワーク認証システム。

【請求項 12】

請求項 8 に記載のネットワーク認証装置と、  
前記ネットワーク認証装置との間で鍵交換処理を行って IP セキュリティ通信

パスを生成し、鍵交換処理により作成した鍵を用いてパケットを暗号化及び復号化し、該 IP セキュリティ通信パスを介して前記ネットワーク認証装置と通信するユーザ端末と、

前記ネットワーク認証装置に接続され、前記ユーザ端末に対してデータを提供する情報サーバと、

前記ネットワーク認証装置に接続され、前記ユーザ端末からの認証要求に従い、前記情報サーバへのアクセスを許可するための認証を行う認証サーバと、  
を備え、

前記認証サーバは、前記ユーザ端末から、ユーザ識別子、パスワード、MAC アドレス、IP v6 アドレス又は該アドレスのインタフェース識別子、前記ユーザ端末と前記認証サーバに格納されている予め定められた同一の鍵のいずれか又は複数を含み認証パラメータを受け取り、該認証パラメータと予め記憶されている認証用データに基づき前記ユーザ端末を認証し、前記ネットワーク認証装置に、認証した前記ユーザ端末から前記情報サーバへのパケットを中継させるネットワーク認証システム。

#### 【発明の詳細な説明】

##### 【0001】

#### 【発明の属する技術分野】

本発明は、ネットワーク認証装置及びネットワーク認証システムに係り、特に、アクセスが許可された端末からのパケットを中継するネットワーク認証装置、及び、ネットワーク認証システムに関する。

##### 【0002】

#### 【従来の技術】

各種情報機器及び通信機器の発達によりネットワークの利用が増え、それに伴い、ネットワークが保持する情報に対する信用を確保するために、ネットワークの利用を制限する情報セキュリティ技術の必要性が認識されている。例えば、外部からの不正な利用者や、利用を許可されていない内部の者であっても、ネットワークに接続されているサーバにアクセスが可能である。これらの不正なアクセスを防止する手段として、ユーザ ID とパスワードを使ったユーザ認証やルータ

等の通信機器によるパケットフィルタリングが知られている（例えば、特許文献 1 参照）。

#### 【0003】

パケットフィルタリングには、同一サブネット内でパケット（フレーム）を中継する L2 スイッチ（例えば、LAN スイッチ）による MAC（Media Access Control）フィルタリングと、異なるサブネット間でパケットをルーティングするルータによる IP フィルタリングが知られている。また、L2（Layer 2）スイッチとルータを切り替えるマルチレイヤスイッチが提案されている。

#### 【0004】

図 28 は、マルチレイヤスイッチによるフィルタリング処理の概略図である。マルチレイヤスイッチは、例えば、L2 スイッチ機能 10 と、ルータ機能 20 と、レイヤー判断部 30 とを備える。L2 スイッチ機能 10 の MAC アドレス処理部 11 は、MAC アドレスフィルタリングテーブル 12 を参照し、MAC アドレス（物理アドレス）に基づきパケットをフィルタリングする。また、ルータ機能 20 の IP アドレス処理部 21 は、IP アドレスフィルタリングテーブル 22 を参照し、IP アドレスに基づきパケットをフィルタリングする。ルータ機能 20 は、さらに MAC ヘッダ除去やホップ数の変更など適宜のルーティング処理を行う場合もある。レイヤー判断部 30 は、例えば、受け取ったパケットの宛先 IP サブネットと入力ポートのサブネットが同一である、又は、宛先ポートと入力ポートが同一 VLAN（Virtual LAN）である等の条件に基づき、L2 スイッチ機能 10 又はルータ機能 20 のいずれかにパケットを中継する。図 28 に示すように、マルチレイヤスイッチは、レイヤー判断部 30 の判断結果に基づき、MAC アドレス又は IP アドレスのいずれか一方のみによりフィルタリングする。したがって、通常の L2 スイッチ及びルータと比較してセキュリティ強度に大きな違いは生じない。

#### 【0005】

また、広域イーサネット（登録商標）サービスが始まり、これを用いて企業と家庭（SOHO、Small Office Home office）を結ぶ広域 VPN（Virtual Private Network）の構築が可能となっている。しかし、広域イーサネット（登録商



標)は、簡単に使える反面、セキュリティ強度が低いという課題がある。

#### 【0006】

さらに、ADSL (Asymmetric Digital Subscriber Line)、ケーブルテレビ等に代表される常時接続ブロードバンドの普及により、リモートオフィス化の要求が増大している。企業の本社と家庭 (SOHO) 又は支店を結ぶ企業イントラネットを、インターネットと IPsec (IP security protocol、IPセキュリティ) を組み合わせたインターネットVPNで安く構築しようというものである。企業イントラネットといっても各事業所には独自のポリシーがあり、同じ企業の社員であっても他の事業所からは特定のユーザからのアクセスのみ許可するのが一般的である。そのため、独自のポリシーに基づくセキュリティ対策、セキュリティシステムが必要となる。しかし、インターネットVPNでは、ルータを介したネットワーク間でVPNを構成するため、MACアドレスによる認証及びフィルタリングはできず、IPv4アドレスでのフィルタリング等が行われている。

#### 【特許文献1】

特開 2002-84306 号公報

#### 【0007】

#### 【発明が解決しようとする課題】

従来の IPv4 (Internet Protocol version 4) アドレスを用いたインターネットの場合、ユーザ端末が移動すると、移動先で DHCP (Dynamic Host Configuration Protocol) サーバから新たに IP アドレスの配布を受け、その度に IP アドレスが変化する。そのため、IP アドレスをユーザ認証やフィルタのパラメータとして使用することができない場合があった。すなわち、従来の IPv4 アドレスによるユーザ認証及びフィルタリングを行うシステムでは、モビリティとセキュリティの両方を確保することが困難であった。また、同一 IPv4 アドレスに成りすました侵入者に対するセキュリティが低いという課題がある。

#### 【0008】

また、例えば、インターネットVPN等のルータを介するネットワークでは、ユーザ端末の MAC アドレスがルータのアドレスに付け替えられるため、装置固有の情報をを用いたユーザ認証、及び、パケットフィルタリングができない課題が

ある。

#### 【0009】

本発明は、以上の点に鑑み、アクセスが許可されていない端末からのアクセス、及び、なりすましによる侵入者からのアクセスを拒否する高セキュリティなネットワークシステムを構築することを目的とする。また、本発明は、IPv6アドレスのインタフェースID部分を活用してセキュリティ強度の高いユーザ認証及びパケットフィルタリングを行うことを目的とする。特に、ルータを介して通信を行うネットワークシステムにおいて、従来のIPv4アドレスによるフィルタリングよりも強度の高いセキュリティシステムを提供することを目的とする。また、本発明は、ユーザ端末の移動に対しても高いセキュリティ強度を有するモビリティの優れたシステムを提供することも目的のひとつである。

#### 【0010】

さらに、本発明は、L2スイッチにIPフィルタリング機能を持たせ、MACアドレス及びIPアドレス等をパラメータとした多段フィルタリングを行い、セキュリティ強度を高くすることを目的とする。本発明は、ユーザID及びパスワードに加えてIPv6 (Internet Protocol version 6) アドレスのインタフェースID及びIKE (Internet Key Exchange)のユーザ認証機能を併用することによりユーザ認証の確度を高めることを目的とする。また、本発明は、広域イーサネット (登録商標)、構内データセンタ、インターネットVPN等のネットワークにおける高セキュリティなネットワークシステムを提供することを目的とする。

#### 【0011】

##### 【課題を解決するための手段】

本発明の第1の解決手段によると、

ユーザ認証を行い、ネットワークを介してユーザ端末と情報サーバ間でパケットを送受信するネットワークシステムにおけるネットワーク認証装置であって、

ユーザ端末及び情報サーバに対してパケットを送受信するネットワークインタフェース部と、

受信したパケットを中継すべき前記ネットワークインタフェース部を示す情報

が登録されるアドレステーブルと、

入力されたパケットを、該パケットの宛先アドレスに基づき、前記アドレステーブルが示すネットワークインタフェース部を介して中継するパケット中継部と、

パケットの中継又は廃棄を示す情報が登録されており、認証されたユーザ端末からのパケットを中継するように情報が更新されるフィルタリングテーブルを有し、前記ネットワークインタフェース部を介して受信したパケットの宛先アドレスに対応する、送信元MACアドレスと送信元IPv6アドレスとの両方の情報に基づき、前記フィルタリングテーブルを参照して条件を判断し、該受信したパケットを前記パケット中継部へ中継する又は廃棄するフィルタリング処理部と、を備えたネットワーク認証装置が提供される。

#### 【0012】

本発明の第2の解決手段によると、

上記ネットワーク認証装置と、

ネットワークを介して前記ネットワーク認証装置に接続されたユーザ端末と、

前記ネットワーク認証装置に接続され、前記ユーザ端末に対してデータを提供する情報サーバと、

前記ネットワーク認証装置に接続され、前記ユーザ端末からの認証要求に従い、前記情報サーバへのアクセスを許可するための認証を行う認証サーバと、を備え、

前記認証サーバは、前記ユーザ端末から、MACアドレス、IPv6アドレス又は該アドレスのインタフェース識別子のいずれか又は複数を含む認証パラメータを受け取り、

該認証パラメータと予め記憶されている認証用データに基づき前記ユーザ端末を認証し、前記ネットワーク認証装置に、認証した前記ユーザ端末から前記情報サーバへのパケットを中継させるネットワーク認証システムが提供される。

#### 【0013】

本発明の第3の解決手段によると、

上記ネットワーク認証装置と、

パケットをルーティングするためのルータと、  
前記ルータ及びネットワークを介して前記ネットワーク認証装置に接続されたユーザ端末と、

前記ネットワーク認証装置に接続され、前記ユーザ端末に対してデータを提供する情報サーバと、

前記ルータに接続され、前記ユーザ端末からの認証要求に従い、前記情報サーバへのアクセスを許可するための認証を行う認証サーバと、  
を備え、

前記認証サーバは、前記ユーザ端末から、ユーザ識別子、パスワード、MAC アドレス、IP v 6 アドレス又は該アドレスのインタフェース識別子のいずれか又は複数を含む認証パラメータを受け取り、

該認証パラメータと予め記憶されている認証用データに基づき前記ユーザ端末を認証し、前記ネットワーク認証装置に、認証した前記ユーザ端末から前記情報サーバへのパケットを中継させるネットワーク認証システムが提供される。

#### 【0014】

本発明の第4の解決手段によると、

通信相手毎に鍵交換処理を行って通信パスを確立し、通信相手毎に鍵交換処理により作成した鍵、及び、通信相手の認証を行うための予め定められた鍵若しくは認証情報を格納するIPセキュリティ制御部、及び、

前記IPセキュリティ制御部により作成された鍵を用いたパケットの暗号化及び復号化機能、及び、パケット改ざんチェック機能、及び、前記IPセキュリティ制御部に記憶されている予め定められた鍵若しくは認証情報に基づく通信相手の認証機能とを有し、通信相手を認証した場合にパケットを前記フィルタリング処理部へ送信し、一方、認証されなかった場合にパケットを廃棄するIPセキュリティ処理部をさらに備えた前記ネットワーク認証装置と、

前記ネットワーク認証装置との間で鍵交換処理を行ってIPセキュリティ通信パスを生成し、鍵交換処理により作成した鍵を用いてパケットを暗号化及び復号化し、該IPセキュリティ通信パスを介して前記ネットワーク認証装置と通信するユーザ端末と、

前記ネットワーク認証装置に接続され、前記ユーザ端末に対してデータを提供する情報サーバと、

前記ネットワーク認証装置に接続され、前記ユーザ端末からの認証要求に従い、前記情報サーバへのアクセスを許可するための認証を行う認証サーバと、  
を備え、

前記認証サーバは、前記ユーザ端末から、ユーザ識別子、パスワード、MAC アドレス、IPv6 アドレス又は該アドレスのインタフェース識別子、前記ユーザ端末と前記認証サーバに格納されている予め定められた同一の鍵のいずれか又は複数を含む認証パラメータを受け取り、該認証パラメータと予め記憶されている認証用データに基づき前記ユーザ端末を認証し、前記ネットワーク認証装置に、認証した前記ユーザ端末から前記情報サーバへのパケットを中継させるネットワーク認証システムが提供される。

#### 【0015】

##### 【発明の実施の形態】

#### 1. ネットワーク認証ノード

図1は、ネットワーク認証システムの基本構成図である。ネットワーク認証システムは、IPv6 (Internet Protocol version 6) で通信可能な認証ノード (ネットワークノード) 100、認証サーバ200、情報サーバ300、情報端末 (ユーザ端末) 400を備える。例えば、情報端末400は、認証ノード100と情報コンセント50を介して接続される。

#### 【0016】

認証ノード100は、情報端末400から送られてきたパケットが、認証サーバ200で認証を受けた情報端末400からのパケットか逐一チェックし、パケットを中継又は廃棄する。例えば、ユーザ認証を受けていない情報端末400から情報サーバ300に送られたパケットは、認証ノード100で廃棄される。認証ノード100の詳細な構成及び処理は後述する。認証サーバ200は、情報端末400からの要求に従ってユーザ認証を行う。認証サーバ200は、ユーザ認証が完了すると認証結果を認証ノード100に通知し、認証を受けた情報端末400からのパケットを中継させる。

## 【0017】

図2は、IPv6認証ノード100の構成図である。認証ノード100は、例えば、パケット中継部110、ネットワークインタフェース部a121～e125、フィルタリング処理部131～135、フィルタ変更指示処理部140、IPv6処理部150、アドレステーブル160を備える。なお、ネットワーク認証システムは、適宜の数のネットワークインタフェース部及びフィルタリング処理部を備えることができる。

## 【0018】

ネットワークインタフェース部a121～e125は、それぞれ異なる端末、サーバ又はネットワークに接続されており、パケットの送受信を行う。パケット中継部110は、パケットを受け取るとパケットの宛先に基づきアドレステーブル160を参照し、アドレステーブル160が示すネットワークインタフェース部a121～e125を介してパケットを送信する。

## 【0019】

図3は、フィルタリング処理部131～135の構成図である。フィルタリング処理部131～135は、それぞれパケット処理部510とフィルタリングテーブル520を備える。パケット処理部510は、ネットワークインタフェース部a121～e125を介してパケットを受け取り、フィルタリングテーブル520の情報に基づいて、パケットの「中継」又は「廃棄」を判断する。パケット処理部510は、「中継」と判断した場合、受け取ったパケットをパケット中継部110へ送り、一方、「廃棄」と判断した場合、当該パケットを廃棄する。

## 【0020】

フィルタリングテーブル520には、パケットの中継又は廃棄を判断するための情報が格納されている。例えば、宛先アドレス、送信元のMACアドレス、及び／又は、IPv6アドレス、及び／又は、IPv6アドレスのインタフェースID（以下、IPv6インタフェースIDを記す）、パケットの中継／廃棄を示す情報が関連して格納されている。フィルタリングテーブル520は、フィルタ変更指示処理部140と接続されており、フィルタ変更指示処理部140により、テーブルの内容が変更される。例えば、初期状態では認証サーバ200宛てに以

外のパケットは廃棄するようにテーブルを構成し、認証サーバ200により認証された端末からのパケットを中継するように、テーブルの内容を適宜変更する。

#### 【0021】

フィルタ変更指示処理部140は、認証サーバ200と通信し、認証サーバ200からフィルタリングテーブル520の状態変更指示を受信する。状態変更指示は、例えば、対象とするエントリの内容と、追加／削除の指示を含む。フィルタ変更指示処理部140は、状態変更指示を受信すると、フィルタリングテーブル520にその指示を反映させる。

#### 【0022】

IPv6処理部150は、ルータ通知プロトコルを用いてユーザ端末400にネットワークIDを通知する。IPv6処理部150は、ルータ通知プロトコルを定期的に配信するが、ユーザ端末400からルータ要請プロトコルを受け取った場合にも同じようにネットワークIDを通知する。

#### 【0023】

なお、本実施の形態における認証ノード100は、例えば、L2で動作するスイッチであり、ルータのようにホップ数の変更等のルーティング処理を行わない。L2で動作するスイッチにMACアドレス及びIPv6アドレスに基づくフィルタリング機能を持たせることにより、シンプルな構成で、セキュリティ強度が高い認証ノードを提供することができる。

#### 【0024】

図4は、認証サーバ200の構成図である。認証サーバ200は、認証受付処理部210と、実際にユーザ認証を行う認証部220を有する。認証受付処理部210は、情報端末400からのユーザ認証要求を受け付ける処理部であり、web認証ではポータルサイトに相当する。認証部220には、例えば、ユーザID（ユーザ識別子）、パスワード、IPv6インタフェースID、MACアドレスが関連付けられたテーブルが事前に認証用データとして格納されている。ユーザID、パスワードに加えてIPv6インタフェースIDを用いることでユーザID及びパスワードの不正使用によるアクセスを防止することが可能となる。さ

らに、認証部 220 には、IKE における通信相手の認証を行うための適宜の認証用データ（例えば、通信相手と同一の予め定められた鍵である `pre-shared key`）が格納されていてもよい。

#### 【0025】

また、認証部 220 は、一般的に使われている RADIUS (Remote Authentication Dial In User Service) や LDAP (Lightweight Directory Access Protocol) 等の認証サーバを併用することもできる。さらに、認証サーバ 200 は、外部装置として扱うだけでなく認証ノード 100 に内蔵させることもできる。

#### 【0026】

情報サーバ 300 は、情報端末 400 に対して提供する情報を格納するサーバである。例えば、ファイルサーバや共有ファイルを有する情報端末等であり、情報端末 400 からの要求に応じてデータを提供する。また、情報サーバ 300 は、情報端末 400 からの要求に応じた演算処理を行う演算装置であってもよい。

#### 【0027】

情報端末 400 は、IPv6 で通信可能な端末である。例えば、Windows (登録商標) XP を OS とするパソコンを用いる事ができる。情報端末 400 は、情報コンセント 50 を介して認証サーバ 200 によりユーザ認証を受け、ネットワーク内部の情報サーバ 300 にアクセスする。

#### 【0028】

(変形例)

図 5 は、認証処理部を内蔵した認証ノードの構成図である。図 5 は、図 1 の認証サーバ 200 の機能を内蔵した認証ノード 2100 である。認証ノード 2100 は、例えば、パケット中継部 110、ネットワークインタフェース部 a121～e125、フィルタリング処理部 131～135、フィルタ変更指示処理部 140、アドレステーブル 160、認証処理部 250 を備える。また、認証ノード 2100 は、IPv6 処理部 150 をさらに備えてもよい。

#### 【0029】

図 6 は、認証処理部 250 の構成図である。認証処理部 250 は認証受付処理部 260 と認証部 270 を有する。なお、認証処理部 250 は、認証受付処理部



250だけを内蔵することもできる。認証受付処理部260及び認証部270の詳細は、図4に示す認証サーバの認証受付処理部210及び認証部220と同様である。認証処理部250は、パケット中継部110から認証要求パケットを受け取り、認証を行う。認証後、認証処理部250は、フィルタ変更指示処理部140にフィルタリングテーブル520の状態変更指示を送る。認証サーバ200の機能を認証ノード2100に内蔵することにより、認証前のパケットを構内に中継されることがなくなり、セキュリティ強度が上がる。

#### 【0030】

次に、IPv6アドレスについて説明する。

図7は、IPv6アドレスのアドレスフォーマットである。IPv6アドレスは、上位64ビットのネットワークIDと下位64ビットのインタフェースIDで構成される。ネットワークIDは、ネットワーク上の通信機器によりルータ通知プロトコルを用いて、情報端末400に通知される。インタフェースIDは、メーカIDと個別IDを含む装置固有のIDである。従って、インタフェースIDは、接続先ネットワークが変わっても不変のIDである。なお、インタフェースID中の「FFFE」は、48ビットのMAC(Media Access Control)アドレスから64ビットのインタフェースIDを作成する場合に、メーカIDと個別IDの間に挿入されるものである。

#### 【0031】

ネットワークに接続した情報端末400は、ルータ要請プロトコル(Router Solicitation)を使って認証ノード100(又はネットワーク内に存在するルータ)からネットワークIDを取得する。認証ノード100は、情報端末400からのルータ要請コマンドに従い、又は定期的に、ルータ通知プロトコル(Router Advertisement)を使って情報端末400にネットワークIDを知らせる。ネットワークIDを取得した情報端末400は、ネットワークIDと自身のインタフェースIDからIPv6アドレスを自動生成する。

#### 【0032】

図8は、フィルタリングテーブル520の構成例(1)を示す図である。フィルタリングテーブル520は、パケットの中継又は廃棄の判断のための情報を格

納しており、各エントリは、宛先アドレス条件フィールド610、送信元アドレス条件フィールド620、中継／廃棄フラグフィールド630を含む。宛先アドレス条件フィールド610には、宛先MACアドレス又は「任意」を意味する情報が登録されている。なお、宛先アドレスとして、IPv6アドレス等の適宜のアドレスを用いてもよい。送信元アドレス条件フィールド620は、送信元MACアドレスフィールド621及び送信元IPv6アドレスフィールド622を含み、それぞれMACアドレス、IPv6アドレス又は「任意」を意味する情報が登録される。なお、本実施の形態においてアドレスの表記は、16進数を用い、0は圧縮表記している。

#### 【0033】

中継／廃棄フラグフィールド630には、パケットの宛先アドレスと送信元アドレスがそれぞれ宛先アドレス条件と送信元アドレス条件に一致した受信パケットを中継すべきか又は廃棄すべきかを示す情報が登録されている。複数のエントリの情報と一致するパケットがあった場合は、テーブルの先頭に近いエントリがそのパケットに適用される。また、一致するエントリが一つもないパケットは、パケット処理部510によりパケット中継部110に送られる。

#### 【0034】

パケット処理部510によるフィルタリングは、MACアドレスによるフィルタリング（MACフィルタリング）と、IPv6アドレスによるフィルタリング（IPv6フィルタリング）を別個に行う独立フィルタリング方式とすることができる。パケット処理部510は、MACフィルタリングする場合は、宛先MACアドレスフィールド610及び送信元MACアドレスフィールド621のAND条件により、中継／廃棄フラグフィールド630の情報に従い「中継」又は「廃棄」を判断する。一方、パケット処理部510は、IPv6フィルタリングする場合は、宛先MACアドレスフィールド610及び送信元IPv6アドレスフィールド622のAND条件により、中継／廃棄フラグフィールド630の情報に従い「中継」又は「廃棄」を判断する。なお、送信元アドレス条件フィールド620にMACアドレスのみが登録されたMACアドレスフィルタリングテーブルと、IPv6アドレスのみが登録されたIPv6アドレスフィルタリングテー

ブルが別々に格納されていてもよい。

#### 【0035】

また、パケット処理部510によるフィルタリングは、MACアドレスとIPv6アドレスにより同時にフィルタリングする一括フィルタリング方式とすることもできる。パケット処理部510は、宛先MACアドレスフィールド610、及び、送信元MACアドレスフィールド621、及び、送信元IPv6アドレスフィールド622のAND条件により、中継／廃棄フラグフィールド630の情報に従い「中継」又は「廃棄」を判断することができる。

#### 【0036】

図9は、フィルタリングテーブル520の構成例(2)を示す図である。フィルタリングテーブル520の各エントリは、宛先アドレス条件フィールド610、送信元アドレス条件フィールド620、中継／廃棄フラグフィールド630を含む。送信元アドレス条件フィールド620は、送信元MACアドレスフィールド621及び送信元IPv6インタフェースIDフィールド623を含み、それぞれMACアドレス、IPv6インタフェースID又は「任意」を意味する情報が登録されている。宛先アドレス条件フィールド610、中継／廃棄フラグフィールド630は上述と同様であるので説明を省略する。

#### 【0037】

図10は、アドレステーブル160の構成例(1)を示す図である。アドレステーブル160の各エントリは、アドレスフィールド161、ネットワークインタフェース部フィールド162を含む。例えば、アドレスフィールド161にはMACアドレスが、インタフェース部フィールド162にはネットワークインタフェース部の識別子がそれぞれ格納される。アドレステーブル160の各エントリは、例えば、パケットを中継する際に、パケットの宛先アドレスに対応するネットワークインタフェース部からパケットを送信することを示している。また、アドレスフィールド161には、IPアドレス等、適宜のアドレスを登録することもできる。

#### 【0038】

また、ルータ要請コマンドのパケットはIPv6処理部150へ中継するよう

にアドレステーブル160を構成する。例えば、アドレスフィールド161を自身のMACアドレス(22:22:00:FF:FF:FF)、ネットワークインタフェース部フィールドを「x」としたエントリを登録する。パケット中継部110は、ネットワークインタフェース部として「x」を取得した場合、当該パケットをIPv6処理部150へ中継する。さらに、宛先アドレスがブロードキャストアドレスであるパケットも、同様にしてIPv6処理部150へ中継させる。IPv6処理部150は、パケットがルータ要請コマンドでない場合、適宜パケットを処理する。

#### 【0039】

なお、パケット中継部110が、受け取ったパケットがルータ要請コマンドであるか判断し、ルータ要請コマンドであればパケットをIPv6処理部150へ中継するようにしてもよい。ルータ要請コマンドでない場合、パケット中継部110は、予め定められたポリシーに従いパケットを廃棄する、又は、パケットを全てのネットワークインタフェース部から送信する。

#### 【0040】

図11は、パケット処理部510の処理の詳細説明図である。

パケット処理部510は、ネットワークインタフェース部a121～e125からパケットを受け取ると、受け取ったパケットの中からフィルタリング対象となるアドレス部を抽出する(S101、S102)。この例では、パケット処理部510は、受け取ったパケットから、宛先MACアドレスと送信元MACアドレスと送信元IPv6アドレスをそれぞれ同時に抽出することを示すが、これに限られず適宜の方法により、フィルタリング対象となる複数個の情報を抽出してもよい。

#### 【0041】

次に、パケット処理部510は、例えば、図8に示すようなフィルタリングテーブル520を参照して、抽出したアドレス部とフィルタリングテーブル520をそれぞれ比較し、比較結果として中継又は廃棄を示す情報を取得する(S103、S104)。パケット処理部510は、取得した比較結果のAND条件(S105)により、比較結果の全てが「中継」だった場合、入力したパケットをパ

ケット中継部110へ送り、一方、比較結果の一つでも「廃棄」だった場合、入力したケットを廃棄する（S106）。

#### 【0042】

また、ケット処理部510は、ステップS101、S102で抽出したアドレス部とフィルタリングテーブル520をそれぞれ比較し、各アドレスのAND条件により一括して中継又は廃棄を示す情報を取得してもよい。すなわち、MACフィルタリングとIPv6フィルタリングを独立に行うこともできるし、宛先MACアドレス、送信元MACアドレス、送信元IPv6アドレスのAND条件により、中継又は廃棄を判断する一括フィルタリング方式とすることもできる。

#### 【0043】

図12は、フィルタリング処理部131～135の他の構成図である。図12に示すフィルタリング処理部131～135は、MACフィルタリング、IPv6フィルタリングを順番に行うパイプライン型フィルタリング処理部である。フィルタリング処理部131～135は、それぞれMACアドレス処理部530、IPv6アドレス処理部540、MACアドレスフィルタリングテーブル550、IPv6アドレスフィルタリングテーブル560を備える。上述のフィルタリング処理部131～135が、複数のパラメータを並行してチェックする並行フィルタリング方式であるのに対して、図12に示すフィルタリング処理部131～135は、MACアドレス、IPv6アドレスを別個にチェックする2段フィルタリング方式である。

#### 【0044】

MACアドレス処理部530は、ネットワークインタフェース部a121～e125からケットを受け取ると、受け取ったケットから宛先アドレスと送信元MACアドレスを抽出し、MACアドレスフィルタリングテーブル550を参照してケットの「中継」又は「廃棄」を判断する。MACアドレス処理部530は、ケットの「中継」と判断した場合、受け取ったケットをIPv6アドレス処理部540へ送り、一方、ケットの「廃棄」と判断した場合、受け取ったケットを廃棄する。

#### 【0045】

IPv6 アドレス処理部 540 は、MAC アドレス処理部 530 からパケットを受け取ると、受け取ったパケットから宛先アドレスと送信元 IPv6 アドレスを抽出し、IPv6 アドレスフィルタリングテーブル 560 を参照してパケットの「中継」又は「廃棄」を判断する。IPv6 アドレス処理部 530 は、パケットの「中継」と判断した場合、受け取ったパケットをパケット中継部 110 へ送り、一方、パケットの「廃棄」と判断した場合、受け取ったパケットを廃棄する。なお、図 12 に示すフィルタリング処理部 510 は、MAC アドレス、IPv6 アドレスの順にフィルタリングしているが、逆の順にフィルタリングする構成としてもよい。

#### 【0046】

図 13 は、MAC アドレスフィルタリングテーブル 550 及び IPv6 アドレスフィルタリングテーブル 560 の構成図である。MAC アドレスフィルタリングテーブル 550、及び、IPv6 アドレスフィルタリングテーブル 560 は、図 8 に示すフィルタリングテーブル 520 の送信元 MAC アドレスフィールド 621 と送信元 IPv6 アドレスフィールド 622 を独立して構成したテーブルである。図 13 (a) に示す MAC アドレスフィルタリングテーブル 550 は、宛先アドレス条件フィールド 610、送信元 MAC アドレス条件フィールド 621、中継／廃棄フラグフィールド 630 を含む。図 13 (b) に示す IPv6 アドレスフィルタリングテーブル 560 は、宛先アドレス条件フィールド 610、送信元 IPv6 アドレス条件フィールド 622、中継／廃棄フラグフィールド 630 を含む。なお、送信元 IPv6 アドレスフィールド 622 には、IPv6 インタフェース ID が登録されてもよい。また、宛先アドレスフィールド 610 には、IPv6 アドレスが登録されてもよい。

#### 【0047】

MAC アドレスフィルタリングテーブル 550 及び IPv6 アドレスフィルタリングテーブル 560 は、図 8 又は図 9 に示すフィルタリングテーブル 520 と同様の構成として一つのテーブルとすることもできる。この場合、MAC アドレス処理部 530 及び IPv6 アドレス処理部 540 は、送信元アドレスフィールド 620 の MAC アドレス又は IPv6 アドレスのいずれかを参照して、パケッ

トの「中継」又は「廃棄」を判断する。

【0048】

2. 広域イーサネット（登録商標）への適用事例及び動作例

図14は、広域イーサネット（登録商標）網におけるネットワーク認証システムの構成図である。図14に示すシステムは、通信事業者が提供している広域イーサネット（登録商標）網を使用して、企業等が社内イントラネットを構築した事例である。広域イーサネット（登録商標）網サービスは、通常LANスイッチ（L2スイッチ）で構成したL2サービスを提供しており、各サイトは、フルメッシュでそれぞれのサイトが接続されているように動作する。以下、本実施の形態におけるネットワーク認証システムの動作例を、広域イーサネット（登録商標）網を用いて説明する。

【0049】

ネットワーク認証システムは、サイトA～Dが広域イーサネット（登録商標）網600を介してすべてL2で結ばれており、あたかも全体が構内LANのように動作する。サイトAは、回線終端装置610を介して広域イーサネット（登録商標）網600に接続されているネットワークノード100と、認証サーバ200と、ファイルサーバ（情報サーバ）300を備える。また、ネットワークノード100は、パケット中継部110、ネットワークインタフェース部a121～e125、フィルタリング処理部131～135、ファイル変更指示処理部140、IPv6処理部150、アドレステーブル160を有する。フィルタリング処理部131～135は、MACアドレス処理部530及びIPv6アドレス処理部540を備えてもよい。

【0050】

サイトDは、回線終端装置620を介して広域イーサネット（登録商標）網600に接続されているユーザ端末400を有する。サイトB及びCは、回線終端装置を介して広域イーサネット（登録商標）網600に接続され、例えば、ネットワークノード、LANスイッチ、ユーザ端末、認証サーバ、ファイルサーバ等を有する。

【0051】

サイト A では、例えば、広域イーサネット（登録商標）網 6 0 0 はネットワークノード 1 0 0 のネットワークインタフェース部 b 1 2 2 に、認証サーバ 2 0 0 はネットワークインタフェース部 c 1 2 3 に、ファイルサーバ 3 0 0 はネットワークインタフェース部 d 1 2 4 に、それぞれ接続されている。また、ネットワークノード 1 0 0 の広域イーサネット（登録商標）網 6 0 0 側と認証サーバ 2 0 0 、ファイルサーバ 3 0 0 側は全て同一 I P サブネットアドレスが割り当ててある。従って、I P サブネットをまたぐときに使うルータは不要である。

#### 【 0 0 5 2 】

サイト C 及びサイト D のユーザ端末は、広域イーサネット（登録商標）網 6 0 0 を介してサイト A のファイルサーバ 3 0 0 にアクセス可能である。この場合、ユーザ認証は、ユーザ端末（E n d システム）とサイト単位で行われる。例えば、サイト A の認証サーバ 2 0 0 で認証されたユーザ端末は、サイト A 内の全てのサーバにアクセス可能となる。

#### 【 0 0 5 3 】

なお、広域イーサネット（登録商標）では VLAN-Tag 付きイーサネット（登録商標）パケットが広く使われている。フィルタリング処理部 1 3 1 ～ 1 3 5 は、標準イーサネット（登録商標）だけでなく VLAN-Tag 付きイーサネット（登録商標）パケットもフィルタリング可能である。

#### 【 0 0 5 4 】

次に、サイト D のユーザ端末 4 0 0 が、サイト A のファイルサーバ 3 0 0 だけをアクセス可能とする場合について説明する。サイト A とサイト D は V L A N (V irtual LAN) 1、サイト A、B、C は V L A N 2 として予め設定されている。また、ネットワークノード 1 0 0 の広域イーサネット（登録商標）6 0 0 側のフィルタリング処理部 1 3 2 には、例えば、図 8 に示すようなフィルタリングテーブルが登録されている。例えば、ブロードキャストアドレス (FF:FF:FF:FF:FF:FF)、自ネットワークノード 1 0 0 (22:22:00:FF:FF:FF)、認証サーバ 2 0 0 (22:22:00:11:11:11) を宛先とするパケットのみ中継するように構成されている。また、ネットワークノード 1 0 0 の認証サーバ側、ファイルサーバ側のフィルタリング処理部 1 3 3 及び 1 3 4 のテーブルには何も登録されていない。



## 【0055】

まず、サイトDのユーザ端末400が、IPv6アドレスを生成する処理について説明する。ユーザ端末400は、広域イーサネット（登録商標）網600に接続されると、ネットワークIDを取得するために「ルータ要請コマンド」をブロードキャストする。この時、ルータ要請コマンドを含むパケットの宛先MACアドレスは、ブロードキャストアドレス(FF:FF:FF:FF:FF:FF)として送信される。ブロードキャストされたルータ要請コマンドは、VLAN1で制限されてサイトAだけに届く。

## 【0056】

サイトAのネットワークノード100のフィルタリング処理部132は、ネットワークインタフェース部b122を介して、ルータ要請コマンドを含むパケットを受け取る。フィルタリング処理部132のMACアドレス処理部530は、受け取ったパケットの宛先MACアドレス及び送信元MACアドレスに基づき、フィルタリングテーブル520を参照し、パケットの中継又は廃棄を判断する。宛先MACアドレスがブロードキャストアドレス、送信元MACアドレスがユーザ端末400と一致するエントリは#3及び#4であり、MACアドレス処理部530は、テーブルの上位にある#3のエントリを参照する。#3のエントリの中継／廃棄フラグフィールド630はパケットの「中継」を示している。したがって、MACアドレス処理部530は、当該パケットをIPv6アドレス処理部540へ送る。

## 【0057】

IPv6アドレス処理部540は、パケットを受け取ると、宛先MACアドレス及び送信元IPv6アドレスに基づきフィルタリングテーブル520を参照し、パケットの中継又は廃棄を判断する。宛先MACアドレスがブロードキャストアドレス、送信元IPv6アドレスがユーザ端末400と一致するエントリは#3及び#4である。テーブルの上位のエントリ#3の中継／廃棄フラグフィールド630はパケットの「中継」を示している。したがって、IPv6アドレス処理部540は、パケットの中継と判断し、当該パケットをパケット中継部110へ送る。

## 【0058】

パケット中継部110は、フィルタリング処理部132からパケットを受け取ると、まず、アドレステーブル160を参照し、送信元MACアドレスが一致するエントリが存在するか検索する。なお、アドレステーブル160には、図10に示すエントリが予め登録されている。パケット中継部110は、該当するエントリがアドレステーブル160にない場合、送信元MACアドレス及びルータ要請コマンドを受け取ったネットワークインタフェース部の識別子をアドレステーブル160に追加する。

## 【0059】

図15は、ユーザ端末400のエントリが追加されたアドレステーブル160の構成図である。図10に示すアドレステーブル160には、送信元であるユーザ端末400のMACアドレス(22:22:FF:00:00:01)と一致するエントリがないため、パケット中継部110は、ユーザ端末400のMACアドレス(22:22:FF:00:00:01)とパケットを受信したネットワークインタフェースb122の識別子「b」を含むエントリを追加する。

## 【0060】

次に、パケット中継部110は、アドレステーブル160を参照し、宛先MACアドレスが一致するエントリが存在するか検索し、パケットを中継するネットワークインタフェース部の識別子を取得する。アドレステーブル160には、ブロードキャストアドレス(FF:FF:FF:FF:FF:FF)のエントリがあるので、パケット中継部110は、中継先として「x」を取得する。パケット中継部110は、取得した中継先が「x」であるので、受け取ったルータ要請コマンドをIPv6処理部150へ中継する。

## 【0061】

IPv6処理部150は、ルータ要請コマンドを受け取ると、ルータ通知コマンドを使い、ユーザ端末400(22:22:FF:00:00:01)を宛先としてネットワークIDを含むパケットをパケット中継部110に送る。パケット中継部110は、上述と同様に、アドレステーブル160を参照して、宛先MACアドレスが一致するエントリを検索する。図15に示すように、宛先であるユーザ端末のアドレ

スのエントリは既に登録されており、パケット中継部110は、中継先としてネットワークインタフェース部の識別子「b」を取得する。パケット中継部110は、取得した中継先「b」に従い、ネットワークIDを含むパケットをネットワークインタフェース部b122を介して、ユーザ端末400に中継する。

#### 【0062】

ユーザ端末400は、ネットワークIDを受信し、受信したネットワークIDと自MACアドレスに基づいて自IPv6アドレスを作成する。ユーザ端末400は、IPv6アドレス作成の後に、サイトAのネットワークノード100に対するユーザ認証を行う。

#### 【0063】

図16は、サイトDのユーザ端末400が、サイトAのファイルサーバ300にアクセスするシーケンス図である。まず、ユーザ端末400が、ユーザ認証を受けずにファイルサーバ300にアクセスを試みた場合の処理について説明する。

#### 【0064】

例えば、サイトDのユーザ端末400から、宛先MACアドレスをファイルサーバ300(22:22:00:22:22:22)とするパケットが送信されたとする(S201)。ネットワークノード100のフィルタリング処理部132は、ネットワークインタフェース部b122を介してファイルサーバ300宛のパケットを受け取る。フィルタリング処理部132のMACアドレス処理部530は、受け取ったパケットの宛先MACアドレス及び送信元MACアドレスに基づき、図8に示すフィルタリングテーブル520を参照し、パケットの中継又は廃棄を判断する。宛先MACアドレスがファイルサーバ300(22:22:00:22:22:22)、送信元MACアドレスがユーザ端末400と一致するエントリは#4であり、中継／廃棄フラグフィールド630はパケットの「廃棄」を示している。したがって、MACアドレス処理部530は、当該パケットを廃棄する。このようにして、ユーザ認証を受けていないユーザ端末400からファイルサーバ300へのアクセスは拒否される。

#### 【0065】

次に、ユーザ認証について説明する。まず、ユーザ端末400は、宛先MACアドレスを認証サーバ200(22:22:00:11:11:11)とする認証要求パケットを送信する(S203)。ネットワークノード100のフィルタリング処理部132は、ネットワークインタフェース部b122を介して認証サーバ200宛のパケットを受け取る。フィルタリング処理部132のMACアドレス処理部530は、上述と同様にフィルタリングテーブル520を参照し、パケットの中継又は廃棄を判断する。宛先MACアドレスが認証サーバ200(22:22:00:11:11:11)、送信元MACアドレスがユーザ端末400であるので、MACアドレス処理部530は、エントリは#1のエントリを参照し、パケットをIPv6アドレス処理部540へ送る(S205)。

#### 【0066】

IPv6処理部540は、パケットを受け取ると、上述と同様にフィルタリングテーブル520を参照し、パケットの中継又は廃棄を判断する。宛先MACアドレスが認証サーバ200(22:22:00:11:11:11)、送信元IPv6アドレスがユーザ端末400であるので、IPv6アドレス処理部540は、エントリは#1のエントリを参照し、当該パケットをパケット中継部110へ送る。

#### 【0067】

パケット中継部110は、パケットを受け取るとアドレステーブル160を参照し、送信元MACアドレスが一致するエントリが存在するか検索する。図15に示すようにアドレステーブル160には、既にユーザ端末400(22:22:FF:00:00:01)のエントリが存在するので、次の処理へ移る。

#### 【0068】

次に、パケット中継部110は、宛先MACアドレス(22:22:00:11:11:11)に基づいてアドレステーブル160を参照し、中継先として「c」を取得する。パケット中継部110は、中継先「c」に従い、ネットワークインタフェース部c123を介して当該認証要求パケットを認証サーバ200に中継する(S207)。このように、フィルタリングテーブル520が中継を示すパケットは、宛先アドレスへ中継される。

#### 【0069】

認証サーバ200は、認証要求パケットを受け取ると、宛先MACアドレスをユーザ端末400(22:22:FF:00:00:01)として、ユーザ認証に必要な認証パラメータの要求パケットを送信する(S209)。

#### 【0070】

認証サーバ200から送信されたパケットは、ネットワークインタフェース部c123を介して、フィルタリング処理部133に送られる。パケットを受け取ったフィルタリング処理部133のMACアドレス処理部530は、フィルタリングテーブル520を参照する。フィルタリング処理部132のフィルタリングテーブル520には何も登録されていないため、MACアドレス処理部530は、IPv6アドレス処理部540へパケットを送る(S211)。IPv6アドレス処理部540も同様に、パケットをパケット中継部110へ送る。パケット中継部110は、上述と同様にアドレステーブル160を参照し、宛先であるユーザ端末のMACアドレス(22:22:FF:00:00:01)に対応する中継先として「b」を取得する。パケット中継部110は、ネットワークインタフェース部b122を介してパケットをユーザ端末400に中継する(S213)。

#### 【0071】

認証パラメータの要求パケットを受信したユーザ端末400は、要求された認証パラメータを含むパケットを、認証サーバ200宛に送信する(S215)。認証パラメータとしては、例えば、ユーザID、パスワード、MACアドレス、IPv6インタフェースID(図中、IPv6-ifIDと記す)、IPv6アドレス等の組み合わせ又はいずれかである。

#### 【0072】

ネットワークノード100のフィルタリング処理部132は、ネットワークインタフェース部b122を介して認証サーバ200宛のパケットを受け取る。フィルタリング処理部132のMACアドレス処理部530及びIPv6アドレス処理部540は、上述のステップS205及びS207の認証要求パケットの中継と同様の処理を行い、ネットワークインタフェース部c123から当該パケットを認証サーバ200に中継する(S217、S219)。

## 【0073】

認証サーバ200は、認証パラメータを含むパケットを受信すると、受信した認証パラメータと予め格納されている認証用データとを比較し、ユーザ認証を行う。ユーザ認証のパラメータとしてユーザIDとパスワードの他にMACアドレス、IPv6インタフェースIDを使用し、ユーザ認証の正確性を高めている。ユーザ認証がされると、認証サーバ200は、ネットワークノード100のフィルタ変更指示処理部140と通信し、状態変更指示を送信する(S221)。状態変更指示は、例えば、宛先アドレスの内容として「任意」、送信元アドレスの内容として認証したユーザ端末400のMACアドレス(22:22:FF:00:00:01)及びIPv6アドレス(2001:200:0:1:2222:FFFF:FE00:1)、パケットの「中継」を示すフラグ、エントリの追加を示すフラグを含む。

## 【0074】

図17は、状態変更指示に従い変更されたフィルタリングテーブル520の構成図である。フィルタ変更指示処理部140は、認証サーバ200から状態変更指示を受け取ると、状態変更指示に含まれるユーザ端末400のMACアドレス(22:22:FF:00:00:01)に基づきアドレステーブル160を参照し、そのMACアドレスに対応するネットワークインタフェース部の識別子「b」を取得する。次に、フィルタ変更指示処理部140は、取得した識別子が「b」であるので、ネットワークインタフェース部b122に対応するフィルタリング処理部132のフィルタリングテーブル520を状態変更指示に従い変更する。図17に示すように、認証サーバ200から送信された状態変更指示に応じたエントリが#1に追加される。このエントリが追加されることで、ユーザ端末400からファイルサーバ300等のネットワークノード100に接続されている機器へのパケットは中継されることになる。

## 【0075】

なお、認証サーバ200は、状態変更指示を含むパケットをネットワークノード100宛てに送信し、パケット中継部110は、受け取ったパケットが状態変更指示であるか判断してパケットを中継するように構成してもよい。例えば、自MACアドレス宛のパケットが、状態変更指示を含む場合、受け取ったパケット

をフィルタ変更指示処理部140に中継し、一方、ルータ要請コマンドの場合、受け取ったパケットをIPv6処理部150に中継するように構成してもよい。

#### 【0076】

ユーザ認証が完了した後、ユーザ端末400は、宛先MACアドレスをファイルサーバ300(22:22:00:22:22:22)とするパケット(例えば、ファイルのRead要求)を送信する(S223)。

#### 【0077】

ネットワークノード100のフィルタリング処理部132は、ネットワークインタフェース部b122を介してファイルサーバ300宛のパケットを受け取り、パケットの中継又は廃棄を判断する。送信元MACアドレス(22:22:FF:00:00:01)、及び、送信元IPv6アドレス(2001:200:0:1:2222:FFFF:FE00:1)のエントリがフィルタリングテーブル520の#1に存在するため、フィルタリング処理部132のMACアドレス処理部530は、IPv6アドレス処理部540へパケットを中継し(S225)、IPv6アドレス処理部540は、パケット中継部110へパケットを中継する。

#### 【0078】

パケット中継部110は、アドレステーブル160を参照し、送信元MACアドレスが一致するエントリが存在するか検索する。アドレステーブル160には、既にユーザ端末400のエントリが存在するので、次の処理へ移る。パケット中継部110は、宛先MACアドレス(22:22:00:22:22:22)に基づいてアドレステーブル160を参照し、中継先として「d」を取得する。パケット中継部110は、取得した中継先に従い、ネットワークインタフェース部d124を介して当該パケットをファイルサーバ300に中継する(S227)。

#### 【0079】

ファイルサーバ300は、要求されたデータをユーザ端末400宛に送信する(S229)。送信されたデータは、ネットワークノード100のフィルタリング処理部134に送られる。フィルタリング処理部134は、上述のステップS211及びS213と同様の処理を行い、データをユーザ端末400へ中継する(S231、S233)。

## 【0080】

なお、不正なユーザ端末から同一IPになりすましてファイルサーバ300にパケットが送信された場合、MACアドレス処理部530でのMACフィルタリングにより、当該パケットは廃棄される（S251）。

## 【0081】

上述の実施の形態では、MACアドレス処理部530とIPv6アドレス処理部540により、2段フィルタリングを行っているが、並行してフィルタリングする並行フィルタリング、宛先MACアドレス、送信元MACアドレス、及び、送信元IPv6アドレスに基づく、一括フィルタリングを行うこともできる。また、上述の実施の形態では、MACアドレス及びIPv6アドレスによりフィルタリングしているが、図9に示すようなフィルタリングテーブル520を用いて、MACアドレス及びIPv6インタフェースIDによりフィルタリングすることもできる。

## 【0082】

なお、サイトDのユーザ端末がサイトAのファイルサーバにアクセスする場合等、いずれかのサイトに属するユーザ端末が、他のサイトのファイルサーバにアクセスする場合も、上述と同様の処理によりアクセスが可能となる。

## 【0083】

また、宛先アドレスは、MACアドレスを用いる以外にも、IPv6アドレスを用いることもできる。この場合、アドレステーブル160は、IPアドレスに対応してネットワークインタフェース部の識別子を登録すればよい。

## 【0084】

さらに、認証サーバ200とファイルサーバ300を同一IPアドレスにしてユーザ端末400からは1台のように見せることもできる。最初にユーザ端末400は認証サーバ200に対してユーザ認証を受けるが、認証後、同一IPアドレスを使ってファイルサーバ300にアクセスすることを可能にする。そのためにネットワークノード100は、認証前は認証サーバ200に、認証後はファイルサーバ300にパケットを転送する仕掛けを用意する。例えば、ユーザ認証を受けたIPアドレス等を記憶するためのアドレス登録表を用意する。同一IPア



ドレスにすると、ネットワークノードと認証サーバ、ファイルサーバが1台の装置で動いているように見える。従来技術では1台の実サーバで実現する事ができるが、性能が大幅に劣化する。本実施の形態におけるネットワーク認証システムは、このトラフィック性能に対する向上策でもある。

#### 【0085】

### 3. 構内データセンタへの適用事例及び動作例

図18は、構内データセンタにネットワークノードを適用したネットワーク認証システムの構成図である。図18に示すネットワーク認証システムは、データセンタ700と、認証サーバ200と、情報コンセント730を介してネットワーク3に接続されたユーザ端末400と、ルータ710を備える。データセンタ700は、ファイルサーバ300とネットワークノード100を有する。データセンタ700、認証サーバ200、ユーザ端末400は、それぞれネットワーク1、2、3に接続され、ルータ710を介して通信可能である。また、情報コンセント730を増やすためのLANスイッチ720を備えてもよい。

#### 【0086】

ネットワーク1～3は、それぞれ別のIPサブネットになっており、これらはルータ710を介して通信される。ユーザ端末400からデータセンタ700宛てのパケットが送信されると、ユーザ端末400のMACアドレスは、ルータ710で削除されネットワークノード100まで届かない。したがって、ネットワークノード100では、MACフィルタリングをすることができない。また、IPアドレスのなりすましに対するセキュリティ強度が低い。そこで、本実施の形態では、ネットワークノード100は、IPv6アドレスのインタフェースIDに基づき、パケットをフィルタリングする。インタフェースIDは、装置固有のIDであるため、セキュリティ強度を高くすることができる。

#### 【0087】

データセンタ700は、サーバを一箇所にまとめたものであり、ユーザ端末400に対してwebサービスをはじめとする各種サービスを提供する。なお、サーバは、論理的に集中されていれば、物理的に離れていてもよい。サーバとネットワーク1の出入り口は1箇所に絞り、ここにネットワークノード100を配置

し、特定のユーザ端末400のみ構内へのアクセスを可能にする。特定のユーザ端末400からのみサーバにアクセスさせることで、サーバをD o S (Denial of Service) アタックから守る事ができる。また、ネットワークノード100に認証の仕組みを持たせることで、サーバ毎に認証の仕組みを有する必要がなくなる。

#### 【0088】

図19は、フィルタリングテーブル520の構成例(3)を示す図である。フィルタリングテーブル520は、エントリ毎に宛先IP v 6 アドレス条件フィールド611、送信元IP v 6 インタフェースID条件フィールド623、中継／廃棄フラグフィールド630を含む。図19(a)に示すフィルタリングテーブル520は、ネットワークノード100のネットワーク1側のフィルタリング処理部134に登録されている。なお、ネットワークノード100のファイルサーバ300側のフィルタリング処理部131及び132には、テーブルが何も登録されていない。

#### 【0089】

図20は、アドレステーブル160の構成例(2)を示す図である。図20(a)に示すように、ファイルサーバ300、自ネットワークノード100に関するエントリが予めネットワークノード100のアドレステーブル160に登録されている。

#### 【0090】

図21は、ユーザ端末400がデータセンタ700内のファイルサーバ300にアクセスするシーケンス図である。

#### 【0091】

まず、ユーザ端末400は、情報コンセント730を介してネットワーク3に接続されると、ネットワークIDを取得するために「ルータ要請コマンド」をルータ710に送信する(S301)。なお、ユーザ端末400は、宛先をブロードキャストアドレスとして、「ルータ要請コマンド」を送信してもよい。ルータ710は、ユーザ端末400からの「ルータ要請コマンド」を受け取ると、ルータ通知コマンドを使い、ユーザ端末400にネットワークIDを通知する(S30

3)。ユーザ端末400は、ネットワークIDを受信し、受信したネットワークIDと自MACアドレスに基づいて自IPv6アドレスを作成する。

#### 【0092】

ここで、ユーザ端末400から、宛先IPv6アドレスがファイルサーバ300(2001:200:0:3:2222:00FF:FE22:2222)とするパケットが送信された場合(S305)について説明する。ルータ710は、ユーザ端末400からのパケットを受け取り、ファイルサーバ300が属するネットワーク1にルーティングする(S307)。この時、パケットに含まれていたユーザ端末のMACアドレスは、ルータ710によって削除される。

#### 【0093】

ネットワークノード100のフィルタリング処理部134は、ネットワークインタフェース部d124を介してファイルサーバ300宛のパケットを受け取る。フィルタリング処理部134は、受け取ったパケットから、宛先IPv6アドレス及び送信元IPv6アドレスのインタフェースIDを抽出する。次に、フィルタリング処理部134は、宛先IPv6アドレス及び送信元IPv6インタフェースIDに基づき、図19に示すフィルタリングテーブル520を参照し、パケットの中継又は廃棄を判断する。宛先IPv6アドレスがファイルサーバ300、送信元IPv6インタフェースIDがユーザ端末400と一致するエントリは#1であり、中継／廃棄フラグフィールド630はパケットの「廃棄」を示している。したがって、フィルタリング処理部510は、パケットの廃棄と判断し、当該パケットを廃棄する。このようにして、ユーザ認証を受けていないユーザ端末400からファイルサーバ300へのアクセスは拒否される。

#### 【0094】

次に、ユーザ認証について説明する。まず、ユーザ端末400は、宛先IPv6アドレスを認証サーバ200(2001:200:0:2:2222:00FF:FE11:1111)とする認証要求パケットを送信する(S309)。ルータ710は、ネットワーク3を介して認証要求パケットを受け取り、宛先IPv6アドレスに基づいて、認証要求パケットをネットワーク2へルーティングする(S311)。

#### 【0095】

認証サーバ200は、ネットワーク2を介して認証要求パケットを受け取ると、宛先IPv6アドレスをユーザ端末400(2001:200:0:1:2222:FFFF:FE00:1)として、ユーザ認証に必要な認証パラメータの要求パケットを送信する(S313)。ルータ710は、認証パラメータの要求パケットを受け取り、宛先IPv6アドレスに基づいて、受け取ったパケットをネットワーク3へルーティングする(S315)。

#### 【0096】

ネットワーク3を介して認証パラメータの要求パケットを受信したユーザ端末400は、認証パラメータを含むパケットを、認証サーバ200宛に送信する(S317)。認証パラメータとしては、例えば、ユーザID、パスワード、及び、IPv6インタフェースIDである。

#### 【0097】

認証サーバ200は、ルータ710を介して、ユーザ端末400から送信された認証パラメータを含むパケットを受信する(S319)。次に、認証サーバ200は、受信した認証パラメータと予め格納されている認証用データとを比較し、ユーザ認証を行う。ユーザ認証がされると、認証サーバ200は、ネットワークノード100のフィルタ変更指示処理部140と通信し、フィルタ変更指示処理部140に状態変更指示を送信する(S321)。状態変更指示は、例えば、宛先アドレスの内容が「任意」、認証したユーザ端末400のIPv6インタフェースID(2222:FFFF:FE00:1)、パケットの「中継」を示すフラグ、エントリの追加を示すフラグを含む。

#### 【0098】

ネットワークノード100のフィルタ変更指示処理部140は、ルータ710、及び、ネットワークインタフェース部d124を介して、認証サーバ200から送信された状態変更指示を受信する(S323)。

#### 【0099】

フィルタ変更指示処理部140は、状態変更指示を受け取ると、ネットワーク1が接続されているネットワークインタフェース部b124に対応するフィルタリング処理部132のフィルタリングテーブル520を状態変更指示に従い変更

する。図19(b)に示すように、認証サーバ200から送信された状態変更指示に応じたエントリが#1に追加される。このエントリが追加されることで、ユーザ端末400からファイルサーバ300へのパケットは中継されることになる。

#### 【0100】

ユーザ認証が完了した後、ユーザ端末400は、宛先IPv6アドレスをファイルサーバ300(2001:200:0:1:2222:00FF:FE22:2222)とするパケット(例えば、ファイルのRead要求)を送信する(S325)。ルータ710は、宛先IPv6アドレスに基づき、パケットをネットワーク1へルーティングする(S327)。

#### 【0101】

ネットワークノード100のフィルタリング処理部134は、ネットワークインタフェース部d124を介してファイルサーバ300宛のパケットを受け取る。次に、フィルタリング処理部134は、上述と同様に受け取ったパケットの宛先IPv6アドレス、及び、送信元IPv6インタフェースIDに基づき、フィルタリングテーブル520を参照し、パケットの中継又は廃棄を判断する。図19(b)に示すように、フィルタリングテーブルの#1及び#3に該当するエントリが存在するため、フィルタリング処理部134は、テーブルの上位に存在する#1のエントリの中継/廃棄フラグフィールド630を参照し、パケットの中継と判断する。フィルタリング処理部134は、受け取ったパケットを、パケット中継部110へ送る。

#### 【0102】

パケット中継部110は、フィルタリング処理部134からパケットを受け取ると、アドレステーブル160を参照し、送信元MACアドレスが一致するエントリが存在するか検索する。図20(a)に示すアドレステーブル160には、送信元であるユーザ端末400のIPv6インタフェースID(2222:FFFF:FE00:1)と一致するエントリがないため、パケット中継部110は、ユーザ端末400のIPv6インタフェースIDとネットワーク1に接続されているネットワークインタフェースd124の識別子「d」を含むエントリを追加する。図20(b)

) に、ユーザ端末 400 のエントリが追加されたアドレステーブル 160 の構成図を示す。

#### 【0103】

次に、パケット中継部 110 は、宛先 IPv6 インタフェース ID (2222:00FF:FE22:2222) に基づいてアドレステーブル 160 を参照し、中継先として「a」を取得する。パケット中継部は、取得した中継先に従い、ネットワークインタフェース部 a121 を介して当該パケットをファイルサーバ 300 に中継する (S329)。

#### 【0104】

ファイルサーバ 300 は、ユーザ端末 400 からのパケットの内容に従い、ユーザ端末 400 (2001:200:0:1:2222:FFFF:FE00:1) を宛先とするパケットを送信する (S331)。

#### 【0105】

ファイルサーバ 300 から送信されたパケットは、ネットワークインタフェース部 a121 を介して、フィルタリング処理部 131 に送られる。パケットを受け取ったフィルタリング処理部 131 は、フィルタリングテーブル 520 を参照する。フィルタリング処理部 132 のフィルタリングテーブル 520 には何も登録されていないため、フィルタリング処理部 131 は、パケット中継部 110 へパケットを送る。

#### 【0106】

パケット中継部 110 は、上述と同様に、宛先 IPv6 インタフェース ID アドレス (2222:FFFF:FE00:1) に基づいてアドレステーブル 160 を参照し、中継先として「d」を取得する。パケット中継部は、取得した「d」に従い、ネットワークインタフェース部 d124 を介して、当該パケットをユーザ端末 400 に送信する (S333)。ユーザ端末 400 は、ルータ 710 を介して、ファイルサーバ 300 から送信されたパケットを受信する (S335)。なお、ユーザ端末 400 は、ユーザ認証を 1 度受けると、構内データセンタ 700 内の他のファイルサーバへもアクセスすることができる。

#### 【0107】

また、不正なユーザ端末（侵入者）からファイルサーバ300にアクセスをしようとした場合（S351）、端末からのパケットはルータ710により送信元MACアドレスが削除されルーティングされるが（S353）、フィルタリング処理部134でのIPv6インタフェースIDに基づくフィルタリングにより、当該パケットは廃棄される。

#### 【0108】

このように、不正なユーザ端末からのアクセスを拒否することにより、ファイルサーバ300をDOSアタックから守ることができる。また、サーバそのものの認証の仕組みを持つ必要がなく、管理も容易である。

#### 【0109】

### 4. インターネットVPNの事例

図22は、インターネットVPNにおけるネットワーク認証システムの構成図である。ネットワーク認証システムは、IPsec通信が可能なネットワークノード1100、認証サーバ200、ファイルサーバ300を有するサイトEと、IPsec通信が可能なユーザ端末1400を有するサイトFを備える。また、サイトEとサイトFは、回線終端装置810及び820を介して、インターネット800に接続されている。図22に示す図は、通信事業者が提供するインターネット接続サービスを用いて、企業等が社内イントラネットを構築した例である。各サイトは、例えば、IPsecを使ってトンネルで結ばれており、各通信パスはあたかも専用線で結ばれているように通信される。また、パケットは暗号化されて送受信される。

#### 【0110】

図23は、IPsec通信が可能なネットワークノード1100の構成図である。ネットワークノード1100は、パケット中継部110と、ネットワークインタフェース部a121～e125と、フィルタリング処理部131～135と、フィルタ変更指示処理部140と、アドレステーブル160と、さらに、IPsec制御部170と、IPsec処理部183～185を備える。なお、IPsec処理部は、少なくともインターネット800に接続されるネットワークインタフェース部に対応して備えられていればよい。例えば、図23に示すネット

ワーク認証ノード1100では、ネットワークインタフェース部123～125に対応して、IPsec処理部183～185を備えている。これ以外にも、全てのネットワークインタフェース部に対応してIPsec処理部を備える等、適宜IPsec処理部を配置することもできる。

#### 【0111】

IPsec制御部170は、通信相手毎にIKE(Internet Key Exchange)を用いた鍵交換処理を主に行う。IPsec制御部170は、ユーザ端末1400との間で秘密対称鍵を作成し、通信パス(SA:Security Association)をインターネット800上に自動生成する。ネットワークノード1100とユーザ端末1400は、IPsec制御部170により生成されたSAを介して、パケットの送受信を行う。また、IPsec制御部170は、ユーザ端末毎に、秘密対称鍵、pre-shared key又は公開鍵等を記憶したキーテーブルを有する。pre-shared keyは、IPsec制御部170とユーザ端末1400に予め記憶された同一のkey(パスワード)である。

#### 【0112】

図24は、キーテーブルの構成例を示す図である。例えば、ユーザ端末のIPv6アドレスフィールド、予め定められたpre-shared keyフィールド、通信パス生成の際に作成した秘密対称鍵フィールドを含む。キーテーブルは、これ以外にも適宜の構成とすることができる。

#### 【0113】

IPsec処理部183～185は、データの暗号/復号処理(ESP:Encapsulating Security Payload)、パケットが改ざんされていないかを確認するためのパケット認証処理(AH:Authentication Header)を主に行う。また、IPsec制御部170に記憶されているpre-shared key等を用いてIKEにおける通信相手の認証を行う。

#### 【0114】

ユーザ端末1400は、IPsec通信が可能な端末であり、ネットワークノード1100との間にSAを形成し、SAを介して通信を行う。なお、パケット中継部110、ネットワークインタフェース部a121～e125、フィルタリ



ング処理部131～135、フィルタ変更指示処理部140については、上述と同様であるので、その説明を省略する。

#### 【0115】

図25は、フィルタリングテーブル520の構成例(4)を示す図である。図25(a)に示すフィルタリングテーブル520は、インターネット800に接続されているネットワークインタフェース部123に対応するフィルタリング処理部133に登録されている。フィルタリングテーブル520は、各エントリ毎に、宛先IPv6アドレス条件フィールド611、送信元IPv6インタフェースID条件フィールド623、中継/廃棄フラグフィールド630を含む。

#### 【0116】

図26は、アドレステーブル160の構成例(3)を示す図である。例えば、アドレステーブル160には、認証サーバ200、ファイルサーバ300、自ネットワークノード1100に関するエントリが予め登録されている。

#### 【0117】

図27は、インターネットVPNにおけるネットワーク認証システムのシーケンス図である。まず、ユーザ端末1400から、IPsecを使用せずファイルサーバ宛てのパケットが送信された場合の処理について説明する。

#### 【0118】

例えば、ユーザ端末1400は、ファイルサーバ宛てのパケットを送信する(S401)。サイトEのネットワークノード1100のネットワークインタフェース部c123は、インターネット800を介してパケットを受け取り、IPsec処理部183へ送る。IPsec処理部183は、IPsec制御部170に記憶されているPre-shared Keyや公開鍵等を参照し、例えば、Pre-shared Key認証や、公開鍵暗号認証、デジタル署名認証等を行う。ユーザ端末1400から受け取ったパケットはIPsec処理されていないため、IKEにおける認証を受けることができず、IPsec処理部183は、当該パケットを廃棄する。

#### 【0119】

ここで、IKEにおけるPre-shared Keyを用いた認証の一例に

ついて説明する。ユーザ端末1400は、パケットを送信する際に、予め記憶されている `pre-shared key` と自分のID情報（例えば、IPv6アドレス）に基づき所定の計算をした認証値もあわせて送信する。パケットを受け取ったIPsec処理部183は、受け取ったパケットの送信元IPv6アドレス（又は、IPsec通信装置のアドレス）に基づき、IPsec制御部170のキーテーブルから `pre-shared key` を取得する。IPsec処理部183は、取得した `pre-shared key` と送信元IPv6アドレスに基づき所定の計算を行い、計算結果とユーザ端末1400から送信された認証値を比較する。ユーザ端末1400が、IPv6アドレスに対応した `pre-shared key` を使用していない場合、例えば、 `pre-shared key` を知らない場合、比較結果は一致しない。比較結果が一致すると、IPsec処理部183は、パケットをフィルタリング処理部133へ送る。一方、比較結果が一致しない場合、IPsec処理部183は、パケットを廃棄する。なお、上述の認証は一例であり、これ以外にも適宜の認証方式を用いる事ができる。

#### 【0120】

次に、ユーザ端末1400が、ファイルサーバ300にアクセスするまでの処理について説明する。まず、ユーザ端末1400は、ネットワークノード1100との間に、IKEによるIPsec通信パスを確立する（S403）。

#### 【0121】

例えば、ユーザ端末1400は、制御用チャネルISAKMP (Internet security association and key management protocol) SA生成の要求パケットをネットワークノード1100に送信する。ネットワークノード1100のIPsec処理部183は、ネットワークインタフェース部123を介して要求パケットを受け取り、IPsec制御部170へ送る。IPsec制御部170は、要求パケットの送信元と通信受諾／拒否を示す情報が予め登録されているセキュリティポリシーテーブル等を参照し、通信受諾であれば、ユーザ端末1400に受諾通知を送信する。次に、ユーザ端末1400及びIPsec制御部170は、秘密対称鍵の生成、相手が通信受諾の本人であるかの認証（例えば、pre-shared key認証）を行い、ISAKMP SA生成する。さらに、ユーザ端末1400及

び IPsec 制御部 170 は、ISAKMP SA を介して通信し、秘密対称鍵の生成、実際にパケットを送受信するための SA を生成する。なお、IPsec 制御部 170 は、生成した秘密対称鍵をユーザ端末 1400 毎に記憶する。以上の処理により、ユーザ端末 1400 とネットワークノードの間に IPsec 通信パスが確立する。

#### 【0122】

次に、ユーザ端末 1400 は、宛先 IP アドレスを認証サーバ 200 とする認証要求パケットを送信する (S405)。なお、サイト E のネットワーク ID を宛先とするユーザ端末 1400 からのパケットは、ESP 機能により通信パスの確立の際に生成した秘密対称鍵を用いて暗号化され、IPsec 通信パスを介して送信される。

#### 【0123】

ネットワークノード 1100 のネットワークインタフェース部 123 は、IPsec 通信パスを介して認証要求パケットを受け取り、IPsec 処理部 183 に送る。IPsec 処理部 183 は、パケットを受け取ると、パケットの送信元 IPv6 アドレス (又は IPsec 通信装置のアドレス) に基づき、IPsec 制御部 170 のキーテーブルから秘密対称鍵を取得する。IPsec 処理部 183 は、取得した秘密対称鍵を用いて ESP 機能によりパケットを復号化する。次に、IPsec 処理部 183 は、IKE における通信相手の認証を行う。例えば、IPsec 処理部 183 は、上述の pre-shared key を用いた認証を行う。通信相手を認証すると、IPsec 処理部 183 は、認証要求パケットをフィルタリング処理部 133 へ送る (S407)。

#### 【0124】

パケットを受け取ったフィルタリング処理部 133 は、パケットの宛先 IPv6 アドレス、送信元 IPv6 インタフェース ID に基づき、図 25 に示すフィルタリングテーブル 520 を参照し、パケットの中継又は廃棄を判断する。認証要求パケットは、宛先が認証サーバ (2001:200:0:3:2222:00FF:FE11:1111)、送信元 IPv6 インタフェース ID がユーザ端末 1400 (2222:FFFF:FE00:0001) であるので、#1 のエントリに該当し、中継/廃棄フラグフィールドは、「中継」を

示している。したがって、フィルタリング処理部 133 は、パケットをパケット中継部 110 へ送る。

#### 【0125】

パケット中継部 110 は、受け取ったパケットの送信元 IPv6 インタフェース ID を抽出し、抽出した送信元 IPv6 インタフェース ID を含むエントリがアドレステーブル 160 に存在するか検索する。送信元であるユーザ端末 1400 の IPv6 インタフェース ID を含むエントリは存在しないため、パケット中継部 110 は、ユーザ端末 1400 の IPv6 インタフェース ID、及び、ユーザ端末 1400 が接続されているネットワークインタフェース部 123 に対応する識別子「c」を含むエントリを追加する。図 26 (b) に、エントリが追加されたアドレステーブル 160 を示す。

#### 【0126】

また、パケット中継部 110 は、受け取ったパケットの宛先 IPv6 インタフェース ID を抽出し、抽出した IPv6 インタフェース ID に基づきアドレステーブル 160 を参照して、中継先のネットワークインタフェース部の識別子を取得する。認証要求パケットは、宛先 IPv6 インタフェース ID が (2222:00FF:FE11:1111) であるので、中継先として「a」を取得する。パケット中継部 110 は、取得した「a」に従って、受け取ったパケットを、ネットワークインタフェース部 a121 から認証サーバ 200 に送信する (S409)。

#### 【0127】

認証サーバ 200 は、ユーザ端末 1400 から認証要求パケットを受け取ると、ユーザ端末 1400 を宛先として、認証パラメータ要求パケットを送信する (S411)。

#### 【0128】

ネットワークインタフェース部 a121 は、認証サーバ 200 から認証パラメータ要求パケットを受け取り、フィルタリング処理部 131 へ送る。フィルタリング処理部 131 のフィルタリングテーブル 520 には何も登録されていないので、フィルタリング処理部 131 は、パケットをパケット中継部 110 へ送る。

#### 【0129】

パケット中継部 110 は、上述と同様に、アドレステーブル 160 を参照し、パケットの宛先 IPv6 インタフェース ID (2222:FFFF:FE00:1) に基づき、中継先「c」を取得する。パケット中継部 110 は、パケットをネットワークインタフェース部 c 123 に対応した IPsec 処理部 183 へ中継する (S413)。IPsec 処理部 183 は、IPsec 制御部 170 からパケットの宛先 IPv6 アドレスに対応する秘密対称鍵を取得し、秘密対称鍵を用いてパケット中継部 110 から受け取ったパケットを ESP 機能により暗号化する。IPsec 処理部 183 は、暗号化したパケットをネットワークインタフェース部 c 123 を介して、ユーザ端末 1400 に送信する (S414)。

#### 【0130】

ユーザ端末 1400 は、認証パラメータ要求パケットを受信すると、IKE 認証情報、IPv6 インタフェース ID を含むパケットを認証サーバ 200 に送信する (S415)。IKE 認証情報としては、例えば、pre-shared key を用いて所定の計算を行った値を用いることができる。また、IKE 認証情報は、これ以外にも適宜の値、情報を用いてもよい。ネットワークノード 100 の IPsec 処理部 183、フィルタリング処理部 133 は、ステップ S407、S409 と同様の処理により、ユーザ端末 1400 からのパケットを認証サーバ 200 へ中継する (S417、S419)。

#### 【0131】

認証サーバ 200 は、IKE 認証情報、IPv6 インタフェース ID を含むパケットを受け取ると、予め記憶されている情報と比較し、ユーザ認証を行う。ユーザ認証がされると、認証サーバ 200 は、ネットワークノード 1100 のフィルタ変更指示処理部 140 と通信し、フィルタ変更指示処理部 140 に状態変更指示を送信する (S421)。状態変更指示は、例えば、宛先 IPv6 アドレスとして「任意」、送信元 IPv6 インタフェース ID としてユーザ端末 1400 の IPv6 インタフェース ID、及び、パケットの「中継」、エントリの追加を示す情報を含む。

#### 【0132】

フィルタ変更指示処理部 140 は、認証サーバ 200 からの状態変更指示を受

け取ると、状態変更指示に含まれる送信元 I P v 6 インタフェース I D に基づき、アドレステーブル 1 6 0 を参照する。フィルタ変更指示処理部 1 4 0 は、ネットワークインタフェース部の識別子「c」を取得する。フィルタ変更指示処理部 1 4 0 は、状態変更指示に従い、取得した識別子「c」に対応するフィルタリング処理部 1 3 3 のフィルタリングテーブルの内容を変更する。図 2 5 (b) に、状態変更指示に従いエントリが追加されたフィルタリングテーブルの構成図を示す。これにより、ユーザ認証されたユーザ端末 1 4 0 0 と、サイト E 内のファイルサーバ 3 0 0 の通信が可能になる。

#### 【0133】

次に、ユーザ端末 1 4 0 0 は、ファイルサーバを宛先として、例えば、ファイルの R e a d 要求を示すパケットを送信する (S 4 2 3)。ネットワークノード 1 1 0 0 の I P s e c 処理部 1 8 3 は、上述と同様にして、ユーザ端末 1 4 0 0 からのパケットを受け取り、フィルタリング処理部 1 3 3 へ送る (S 4 2 5)。また、フィルタリング処理部 1 3 3 は、上述と同様にして、I P s e c 処理部 1 8 3 から受け取ったパケットをパケット中継部 1 1 0 へ送る。

#### 【0134】

パケット中継部 1 1 0 は、宛先 I P v 6 インタフェース I D に基づきアドレステーブルを参照し、中継先として「b」を取得する。パケット中継部 1 1 0 は、ネットワークインタフェース部 1 2 2 を介して、パケットをファイルサーバ 3 0 0 へ送信する (S 4 2 7)。

#### 【0135】

ファイルサーバ 3 0 0 は、ファイルの R e a d 要求を受け取ると、要求に応じたデータを含むパケットをユーザ端末 1 4 0 0 宛てに送信する (S 4 2 9)。ネットワークインタフェース部 b 1 2 2 は、ファイルサーバ 3 0 0 からパケットを受け取り、フィルタリング処理部 1 3 2 へ送る。ステップ S 4 1 3、S 4 1 4 と同様に、フィルタリング処理部 1 3 2 は受け取ったパケットをパケット中継部 1 1 0 へ送り、さらに、パケット中継部 1 1 0 は I P s e c 処理部 1 3 2 へ送る (S 4 3 1)。I P s e c 処理部 1 3 2 は、パケットを E S P 機能により秘密対称鍵を用いて暗号化し、ネットワークインタフェース部 c 1 2 3 を介してパケット

を送信する（S433）。ユーザ端末1400は、ファイルサーバ300からのパケットを受信し、ESP機能により秘密対称鍵を用いて復号化することにより、データを得ることができる。

#### 【0136】

仮に、不正侵入者が同一IPアドレスに成りすましてファイルサーバ300等にパケットを送信（S451）した場合、不正侵入者の端末はネットワークノード1100とpre-shared keyや公開鍵を共有していないため、パケットを受け取ったIPsec処理部183は、IKEにおける通信相手の認証ができず、当該パケットを廃棄する。

#### 【0137】

ADSLなどの常時接続ブロードバンドにより企業と家庭（SOHO）や支店を結ぶ場合、通信事業者のインターネットVPNを利用するケースが増えている。従来の認証方式では、SOHOは、プロバイダの先にある企業との連携作業によって行なう複雑な認証方式となっている。この複雑な手順を簡素化するのにも、本実施の形態におけるIPアドレスフィルタリングを活用することができる。プロバイダは、企業とは関係無く、必要に応じてプロバイダに加入許可のため認証を行う。その後は、SOHOと企業がVPNで繋がるが、企業側エッジでは最初に、プロバイダ認証とは独立にユーザ認証を行うことができる。

#### 【0138】

以上、広域イーサネット（登録商標）、構内データセンタ、インターネットVPNの事例についてユーザ認証及びパケットフィルタリングについて説明したが、認証及びフィルタリングのパラメータは、それぞれの事例に限定されるものではなく、他の事例及び他のネットワークに対しても用いることができる。

#### 【0139】

##### 【発明の効果】

本発明によると、アクセスが許可されていない端末からのアクセス、及び、なりすましによる侵入者からのアクセスを拒否する高セキュリティなネットワークシステムを構築することができる。また、本発明によると、IPv6アドレスのインタフェースID部分を活用してセキュリティ強度の高いユーザ認証及びパケ

ットフィルタリングを行うことができる。特に、ルータを介して通信を行うネットワークシステムにおいて、従来のIP v 4アドレスによるフィルタリングよりも強度の高いセキュリティシステムを提供することができる。また、本発明によると、ユーザ端末の移動に対しても高いセキュリティ強度を有するモビリティの優れたシステムを提供することができる。

#### 【0140】

さらに、本発明によると、L2スイッチにIPフィルタリング機能を持たせ、MACアドレス及びIPアドレス等をパラメータとした多段フィルタリングを行い、セキュリティ強度を高くすることができる。本発明によると、ユーザID及びパスワードに加えてIP v 6アドレスのインタフェースID及びIKEのユーザ認証機能を併用することによりユーザ認証の確度を高めることができる。また、本発明によると、広域イーサネット（登録商標）、構内データセンタ、インターネットVPN等のネットワークにおける高セキュリティなネットワークシステムを提供することができる。

#### 【図面の簡単な説明】

##### 【図1】

ネットワーク認証システムの基本構成図。

##### 【図2】

IP v 6 認証ノードの構成図。

##### 【図3】

フィルタリング処理部の構成図。

##### 【図4】

認証サーバの構成図。

##### 【図5】

認証処理部を内蔵した認証ノードの構成図。

##### 【図6】

認証処理部の構成図。

##### 【図7】

IP v 6 アドレスのアドレスフォーマット。



**【図 8】**

フィルタリングテーブルの構成例（1）を示す図。

**【図 9】**

フィルタリングテーブルの構成例（2）を示す図。

**【図 1 0】**

アドレステーブルの構成例（1）を示す図。

**【図 1 1】**

パケット処理部の処理の詳細説明図。

**【図 1 2】**

フィルタリング処理部の他の構成図。

**【図 1 3】**

MAC アドレスフィルタリングテーブル及び I P v 6 アドレスフィルタリングテーブルの構成図。

**【図 1 4】**

広域イーサネット（登録商標）網におけるネットワーク認証システムの構成図。

**【図 1 5】**

ユーザ端末のエントリが追加されたアドレステーブルの構成図。

**【図 1 6】**

広域イーサネット（登録商標）網におけるネットワーク認証システムのシーケンス図。

**【図 1 7】**

状態変更指示に従い変更されたフィルタリングテーブルの構成図。

**【図 1 8】**

構内データセンタにネットワークノードを適用したネットワーク認証システムの構成図。

**【図 1 9】**

フィルタリングテーブルの構成例（3）を示す図。

**【図 2 0】**

アドレステーブルの構成例（2）を示す図。

【図 2 1】

構内データセンタにネットワークノードを適用したネットワーク認証システムのシーケンス図。

【図 2 2】

インターネットVPNにおけるネットワーク認証システムの構成図。

【図 2 3】

IPsec通信が可能なネットワークノードの構成図。

【図 2 4】

キーテーブルの構成例を示す図。

【図 2 5】

フィルタリングテーブルの構成例（4）を示す図。

【図 2 6】

アドレステーブルの構成例（3）を示す図。

【図 2 7】

インターネットVPNにおけるネットワーク認証システムのシーケンス図。

【図 2 8】

マルチレイヤスイッチによるフィルタリング処理の概略図。

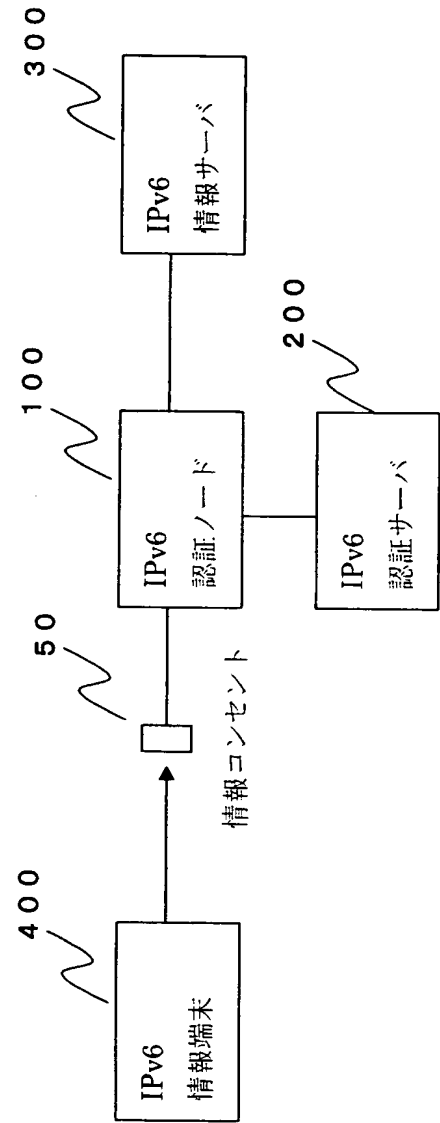
【符号の説明】

- 1 0 0 認証ノード（ネットワークノード）
- 1 1 0 パケット中継部
- 1 2 1～1 2 5 ネットワークインタフェース部 a～e
- 1 3 1～1 3 5 フィルタリング処理部
- 1 4 0 フィルタ変更指示処理部
- 1 5 0 IP v 6 処理部
- 1 6 0 アドレステーブル
- 2 0 0 認証サーバ
- 2 1 0 認証受付処理部
- 2 2 0 認証部

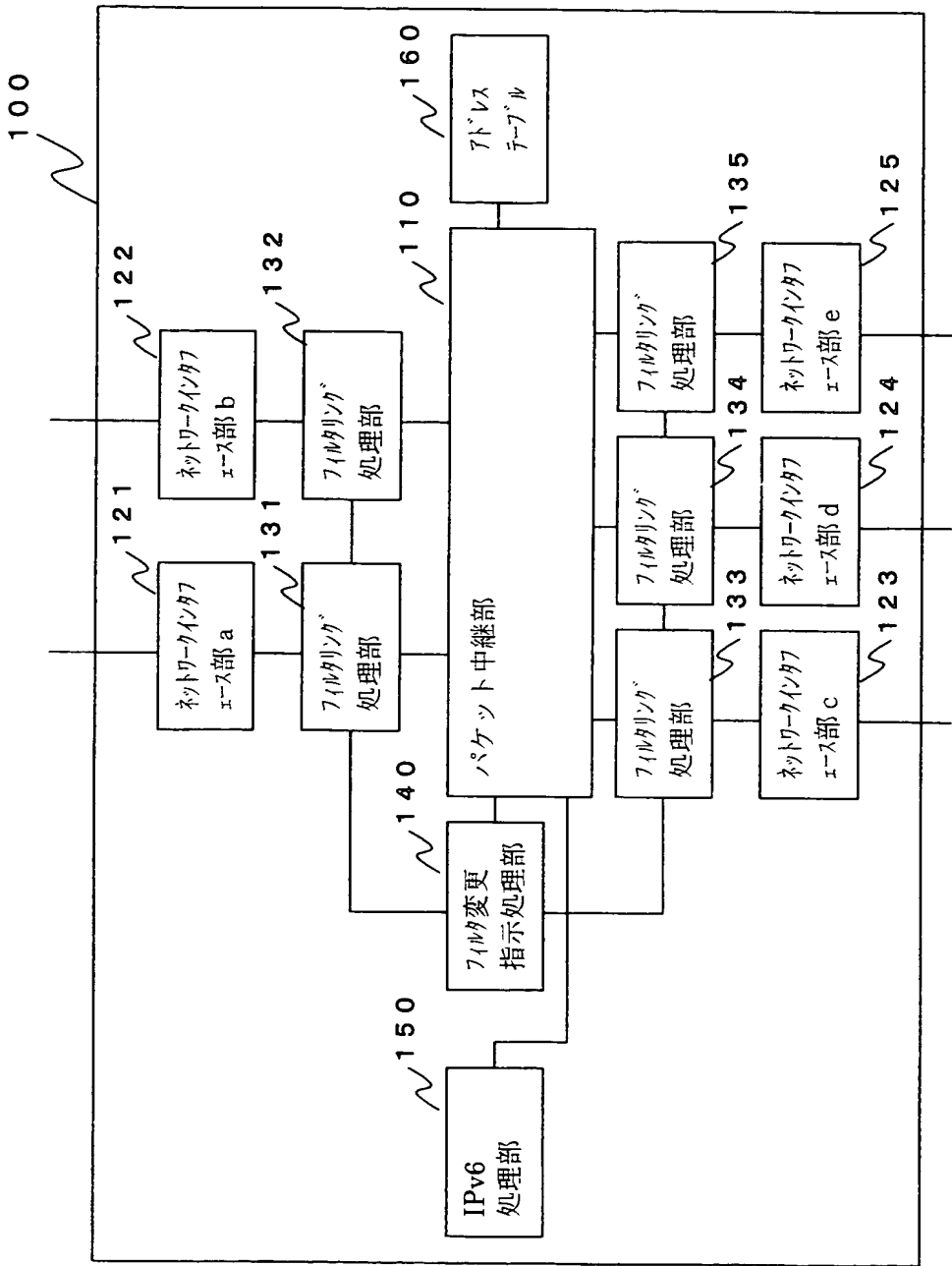
2 5 0 認証処理部  
2 6 0 認証受付処理部  
2 7 0 認証部  
3 0 0 情報サーバ  
4 0 0 情報端末（ユーザ端末）  
5 1 0 パケット処理部  
5 2 0 フィルタリングテーブル  
5 3 0 MACアドレス処理部  
5 4 0 I P v 6 アドレス処理部  
5 5 0 MACアドレスフィルタリングテーブル  
5 6 0 I P v 6 アドレスフィルタリングテーブル  
6 0 0 広域イーサネット（登録商標）網  
6 1 0 回線終端装置  
7 0 0 構内データセンタ  
7 1 0 ルータ  
7 2 0 LANスイッチ  
7 3 0、5 0 情報コンセント  
8 0 0 インターネット  
8 1 0、8 2 0 回線終端装置  
1 1 0 0 ネットワークノード  
1 4 0 0 I P s e c ユーザ端末  
2 1 0 0 認証処理部内蔵ネットワークノード

【書類名】 図面

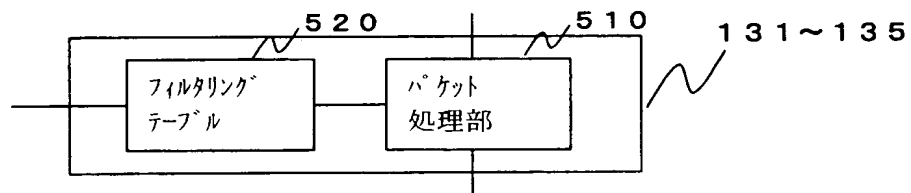
【図 1】



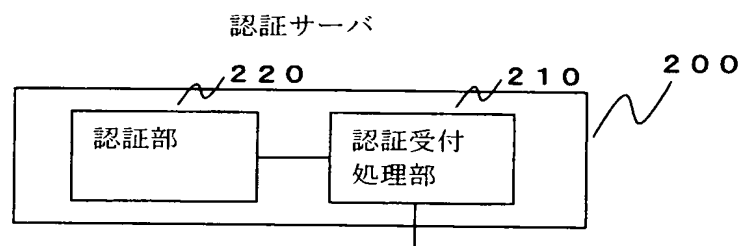
【図 2】



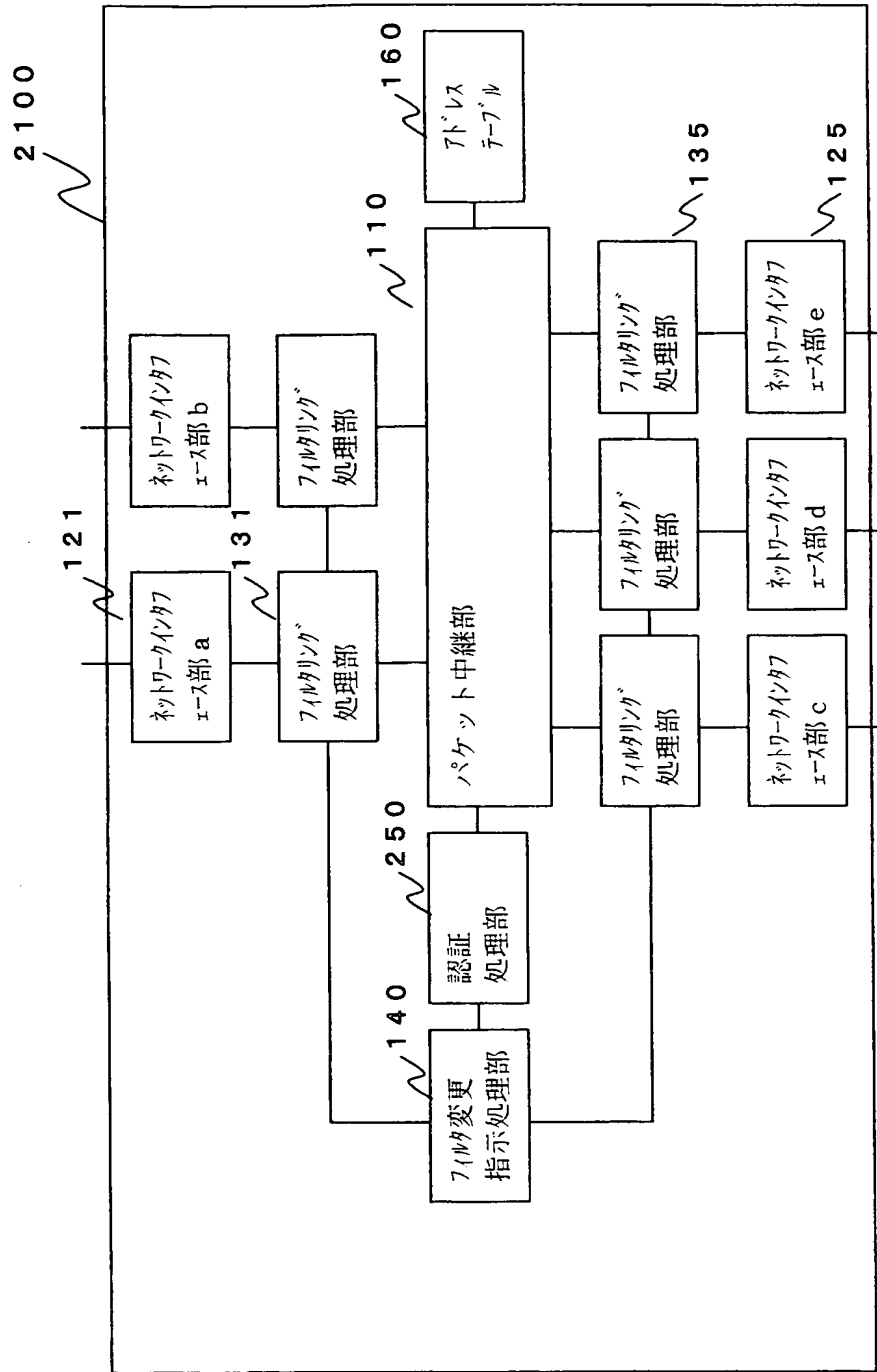
【図 3】



【図 4】

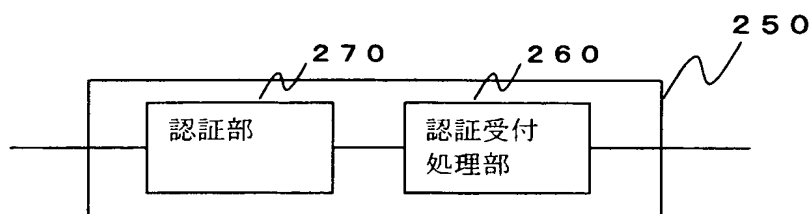


【図 5】

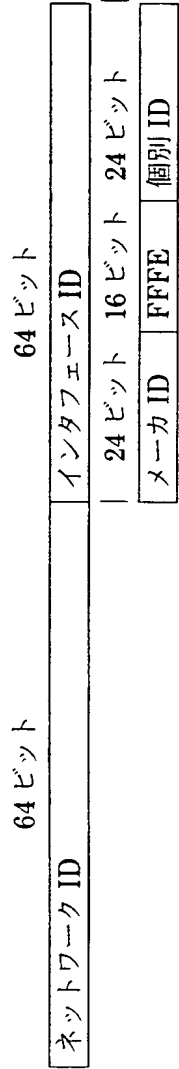




【図 6】



【図 7】



【図 8】

520		610	621	620	622	630
#	宛先 MAC アドレス	送信元アドレス		IPv6 アドレス		中継/廃棄 フラグ
		MAC アドレス				
	1 22:22:00:11:11:11	任意		任意		中継
	2 22:22:00:FF:FF:FF	任意		任意		中継
	3 FF:FF:FF:FF:FF:FF	任意		任意		中継
4	任意	任意		任意		廃棄

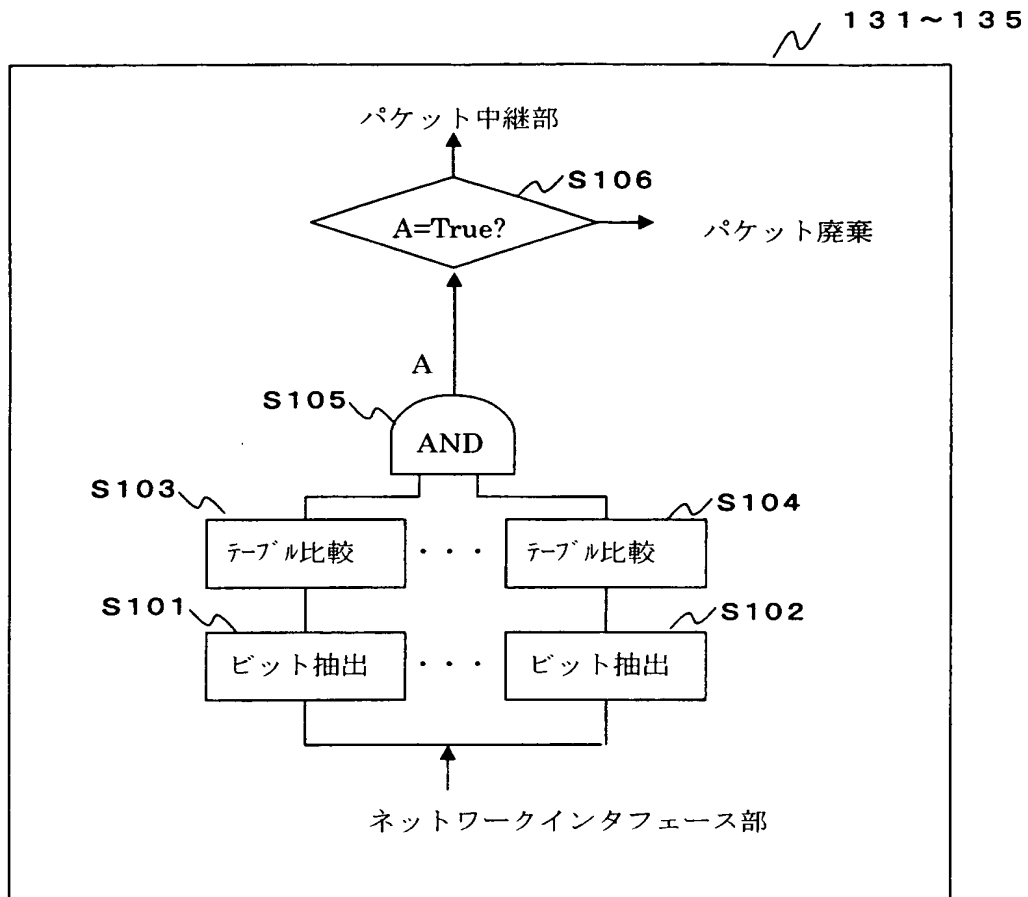
【図 9】

520		610	621	620	623	630
#	宛先 MAC アドレス	送信元アドレス		中継/廃棄		
		MAC アドレス	IPv6 インターフェイス ID	フラグ		
	任意	22:22:FF:00:00:01	2222:FFFF:FE00:1	中継		
	22:22:00:11:11:11	任意	任意	中継		
	22:22:00:FF:FF:FF	任意	任意	中継		
	FF:FF:FF:FF:FF:FF	任意	任意	中継		
5	任意	任意	任意	廃棄		

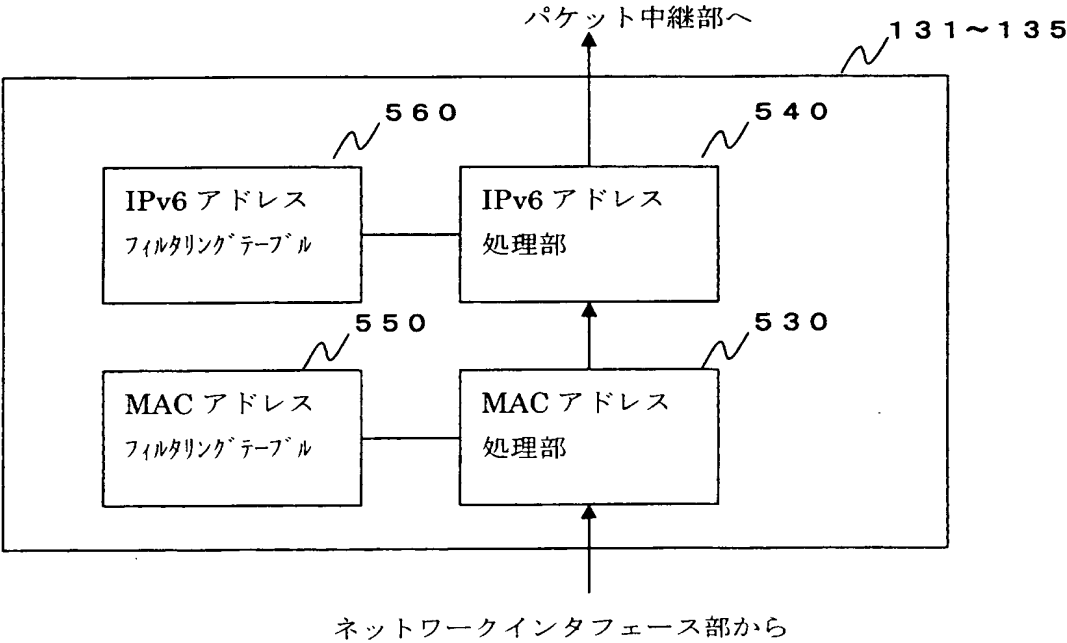
【図 1 0】

MAC アドレス	ネットワーク インタフェース部
22:22:00:11:11:11	c
22:22:FF:22:22:22	d
22:22:00:FF:FF:FF	x
FF:FF:FF:FF:FF:FF	x

【図 11】



【図 12】



【図 13】

550 610 621 630

#	宛先 MAC アドレス	送信元 MAC アドレス	中継/廃棄 フラグ
1	22:22:00:11:11:11	任意	中継
2	22:22:00:FF:FF:FF	任意	中継
3	FF:FF:FF:FF:FF:FF	任意	中継
4	任意	任意	廃棄

(a)

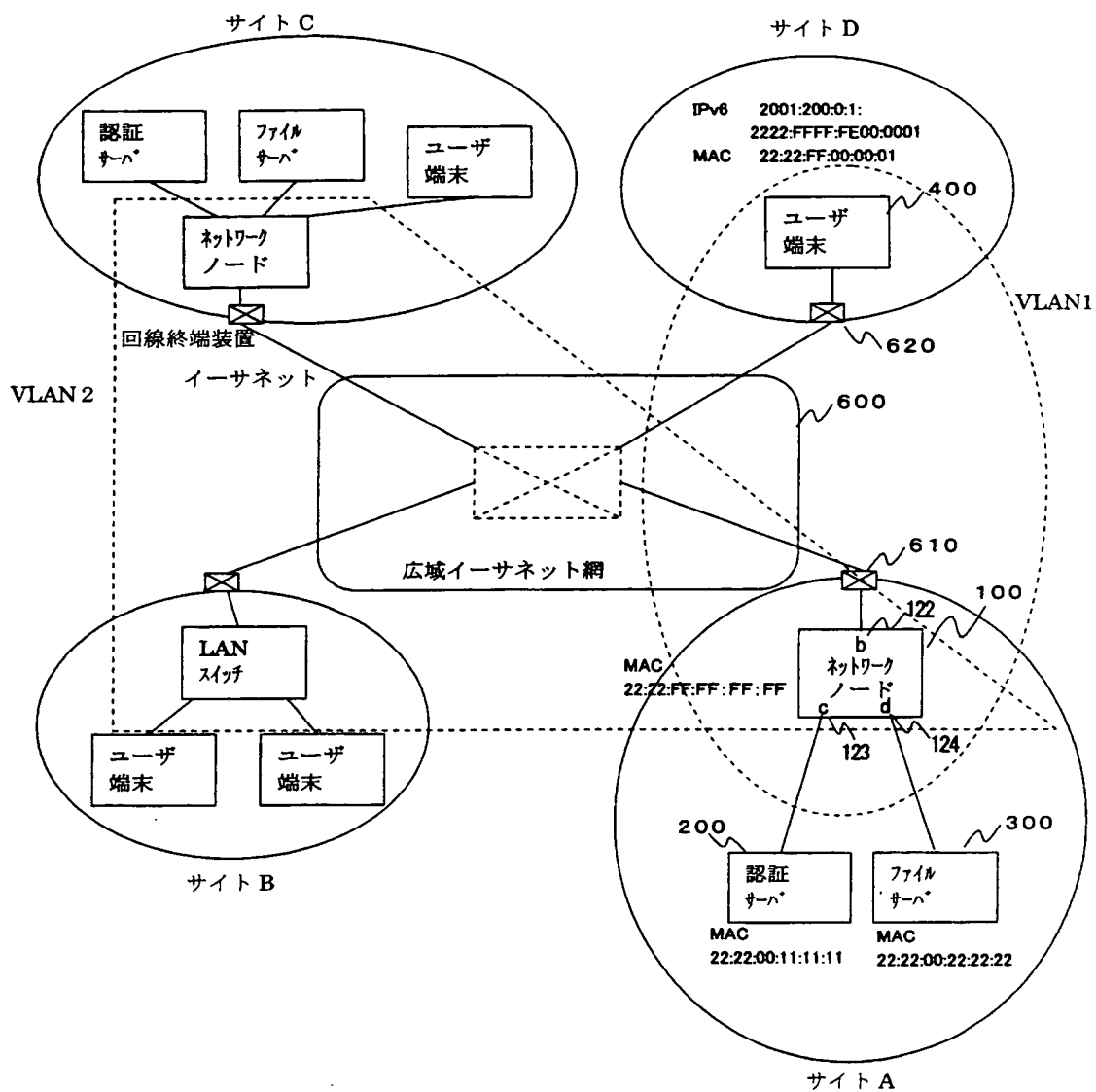
560 610 622 630

#	宛先 MAC アドレス	送信元 IPv6 アドレス	中継/廃棄 フラグ
1	22:22:00:11:11:11	任意	中継
2	22:22:00:FF:FF:FF	任意	中継
3	FF:FF:FF:FF:FF:FF	任意	中継
4	任意	任意	廃棄

(b)



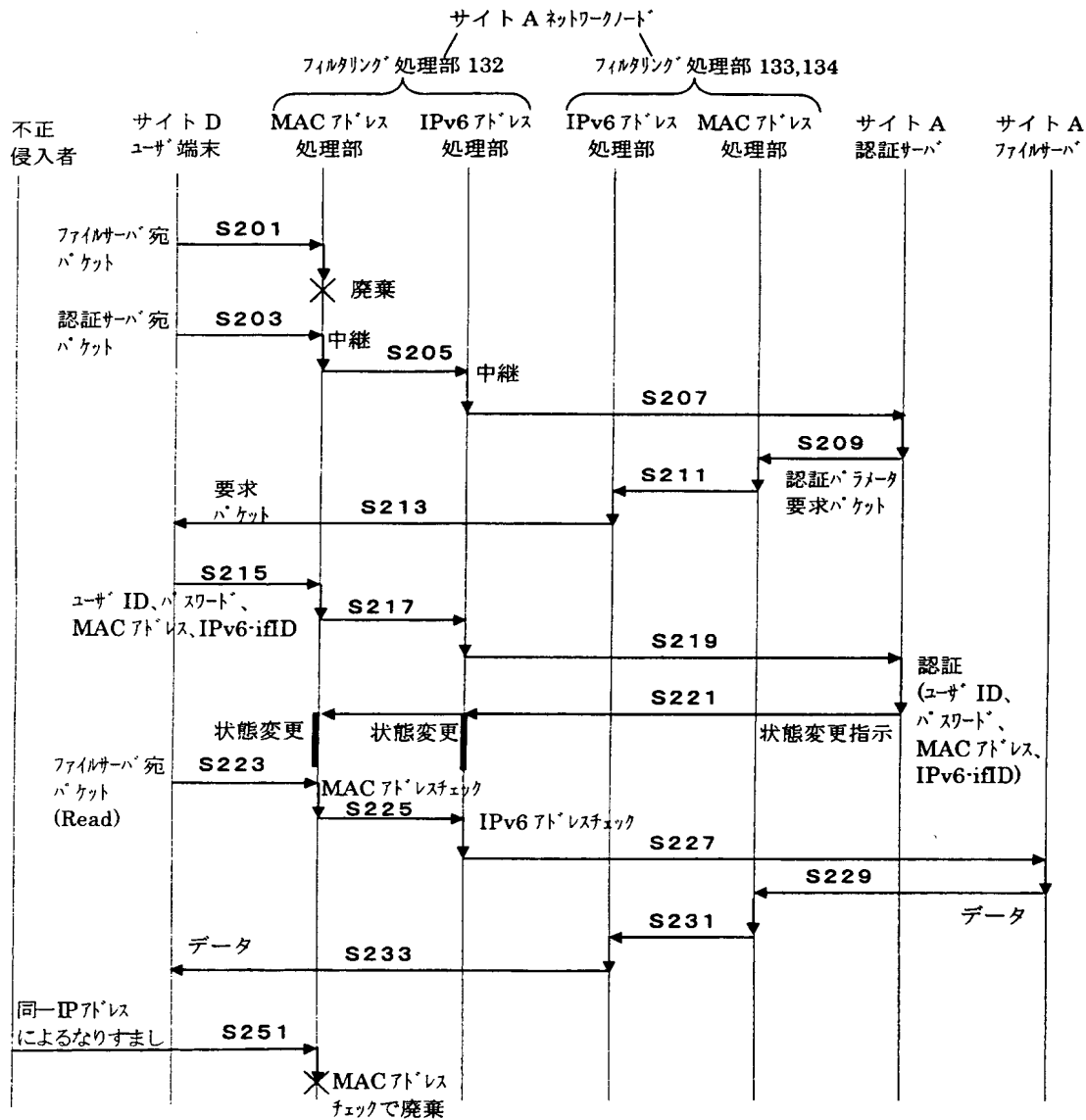
【図 14】



【図 15】

MAC アドレス	ネットワーク インタフェース部
22:22:00:11:11:11	c
22:22:FF:22:22:22	d
22:22:00:FF:FF:FF	x
FF:FF:FF:FF:FF:FF	x
22:22:FF:00:00:01	b

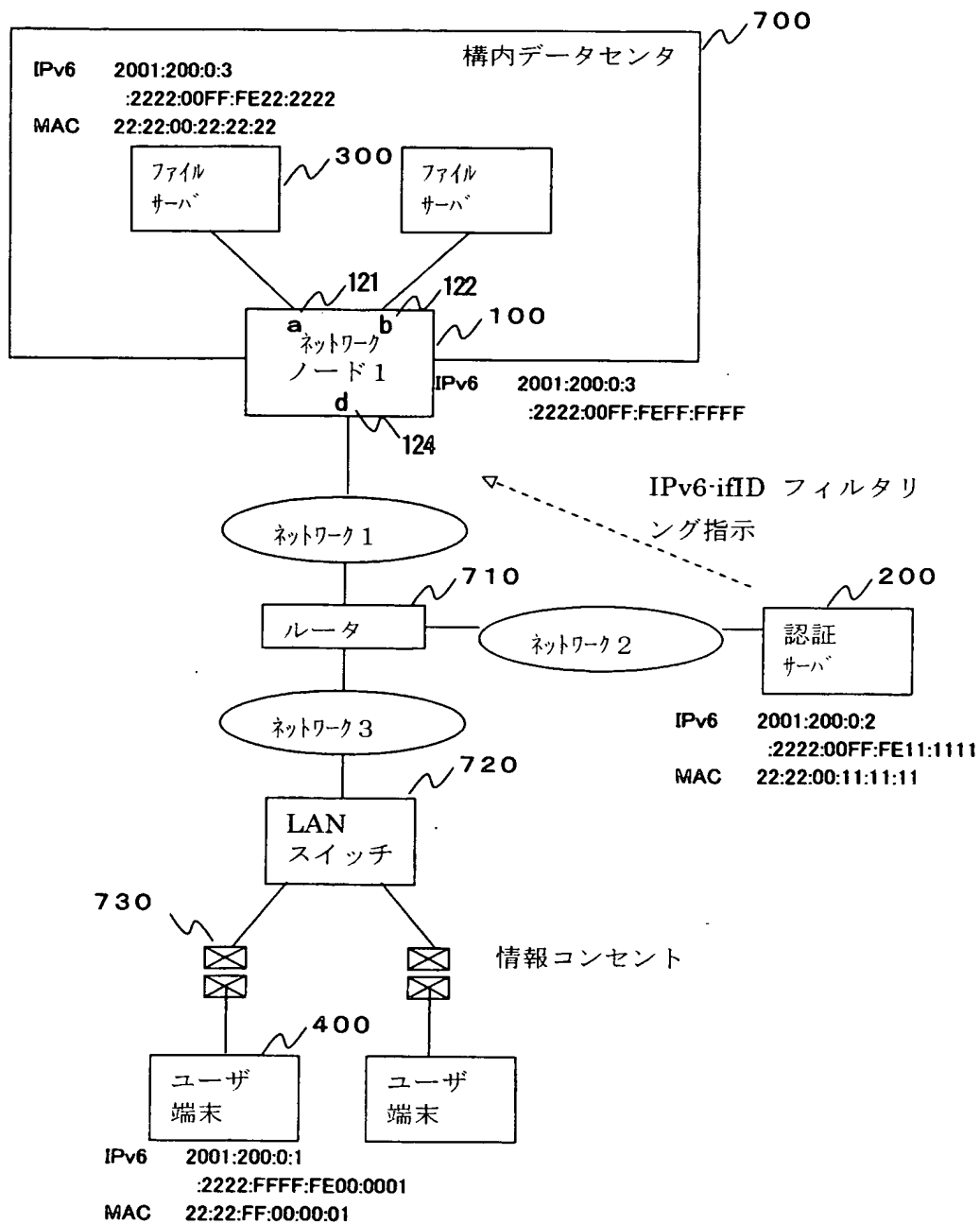
【図 16】



【図 17】

520		610	621	620	622	630
#	宛先 MAC アドレス	送信元アドレス		IPv6 アドレス	中継/廃棄 フラグ	
		MAC アドレス				
1	任意	22:22:FF:00:00:01	2001:200:0:1:2222:FFFF:FE00:1	中継		
2	22:22:00:11:11:11	任意	任意	中継		
3	22:22:00:FF:FF:FF	任意	任意	中継		
4	FF:FF:FF:FF:FF:FF	任意	任意	中継		
5	任意	任意	任意	廃棄		

【図 18】



【図 19】

#	宛先 IPv6 アドレス	送信元 IPv6 インタフェース ID	中継/廃棄 フラグ
1	任意	任意	廃棄

(a)

#	宛先 IPv6 アドレス	送信元 IPv6 インタフェース ID	中継/廃棄 フラグ
1	任意	2222::FFFF:FE00:1	中継
2	任意	任意	廃棄

(b)

【図 20】

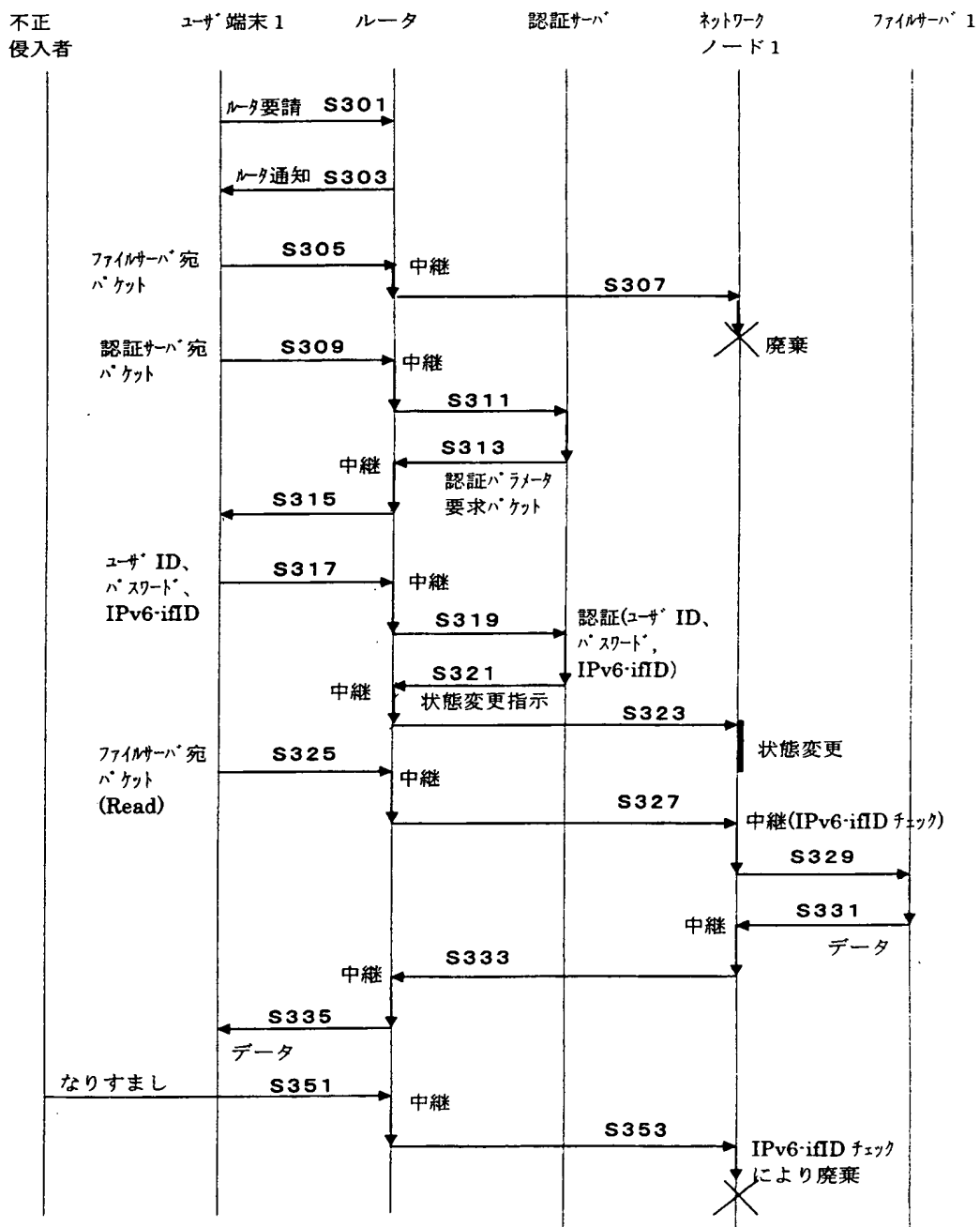
IPv6 インタフェース ID	ネットワークインタフェース部
2222:00FF:FE22:2222	a
2222:00FF:FEFF:FFFF	y

(a)

IPv6 インタフェース ID	ネットワークインタフェース部
2222:00FF:FE22:2222	a
2222:00FF:FEFF:FFFF	y
2222:FFFF:FE00:1	d

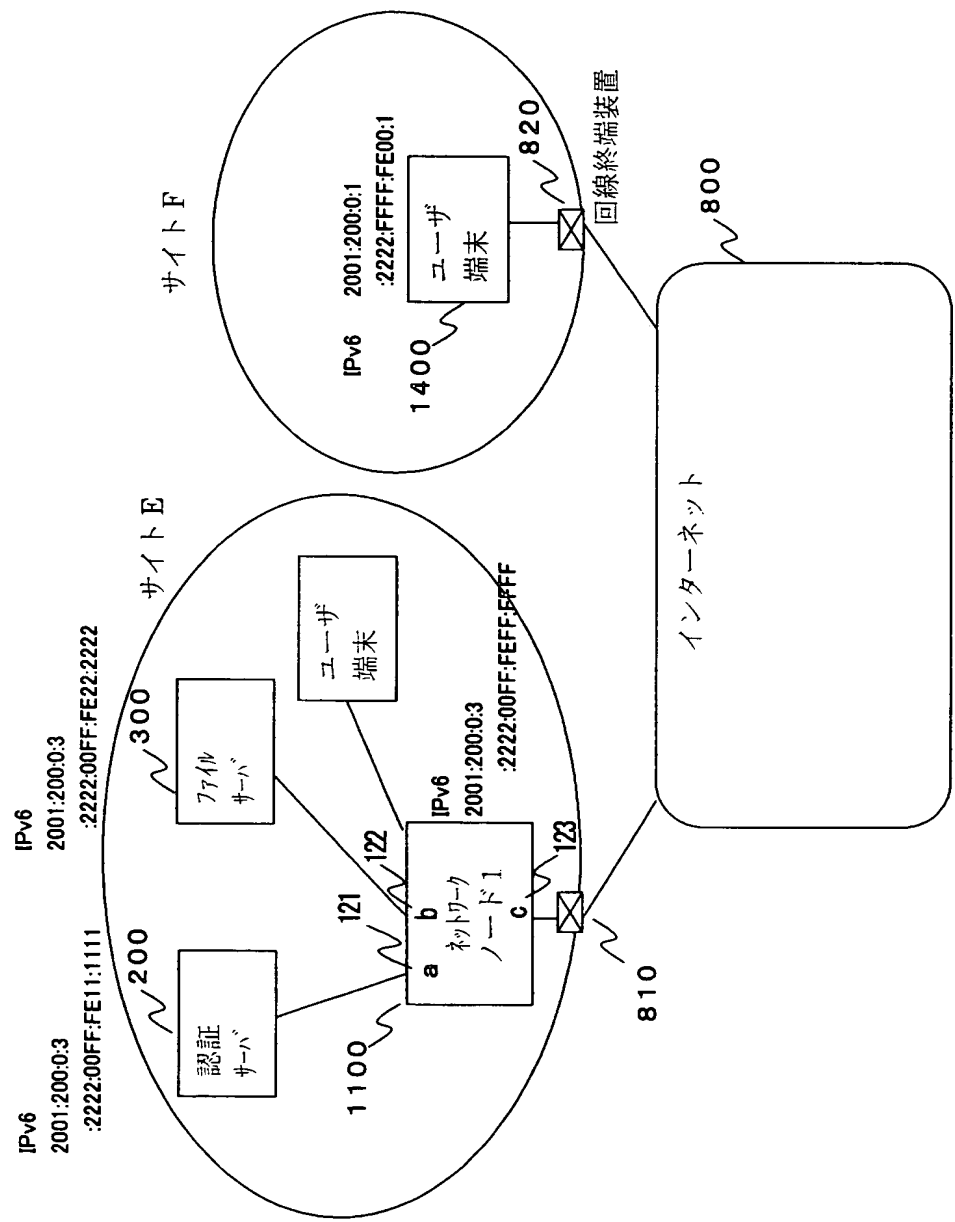
(b)

【図 21】

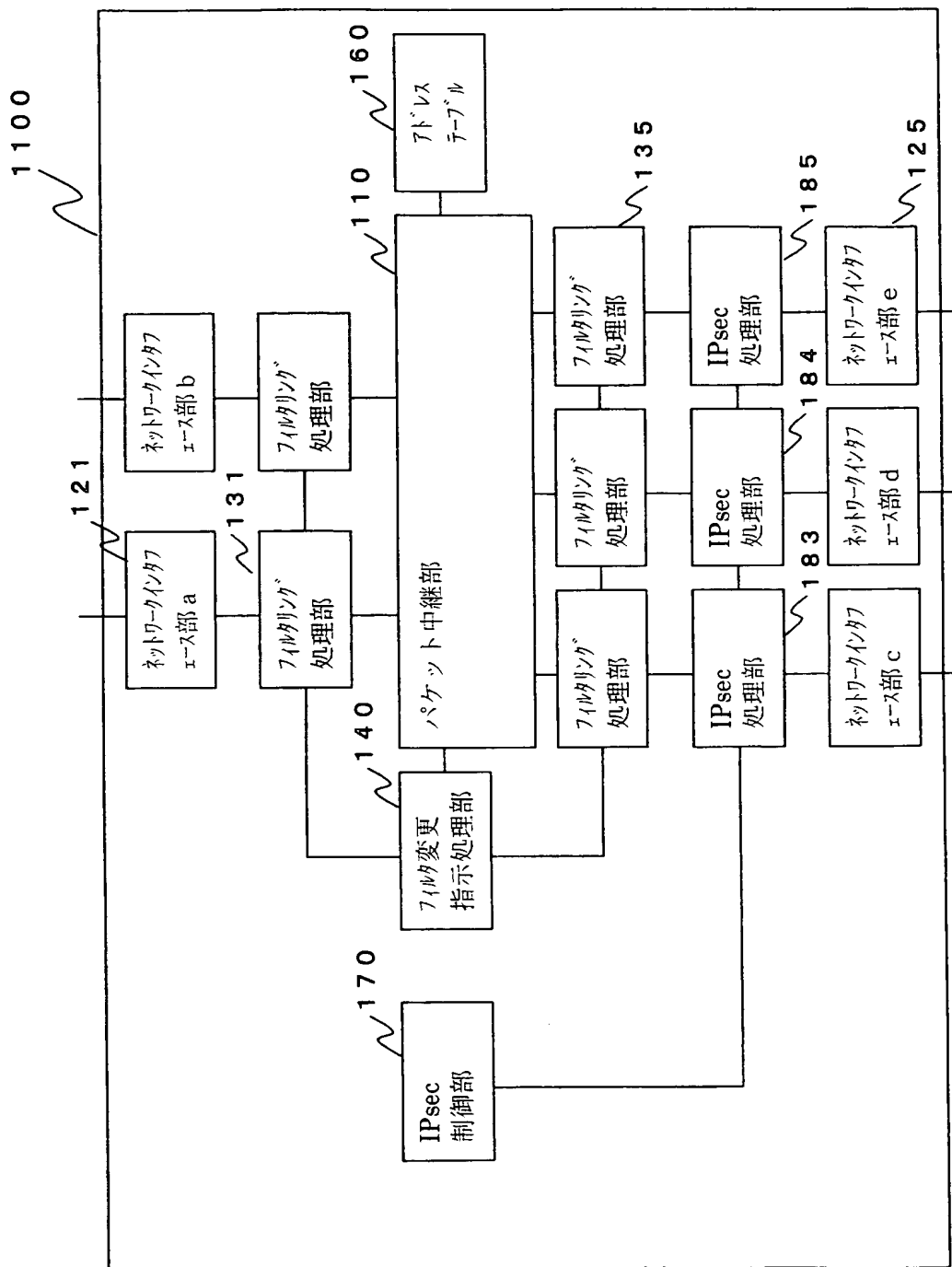




【図 22】



【図 23】



【図 2 4】

ユーザ端末 IPv6 アドレス	Pre-shared key	秘密対称鍵
2001:200:0:1 2222:FFFF:FE00:1	Pre-key a	Secret $\alpha$
⋮	Pre-key b	Secret $\beta$
⋮	⋮	⋮

【図 25】

#	宛先 IPv6 アドレス	送信元 IPv6 インタフェース ID	中継/廃棄 フラグ
1	2001:200:0:3 :2222:00FF:FE11:1111	任意	中継
2	任意	任意	廃棄

(a)

#	宛先 IPv6 アドレス	送信元 IPv6 インタフェース ID	中継/廃棄 フラグ
1	任意	2222:FFFF:FE00:1	中継
2	2001:200:0:3 :2222:00FF:FE11:1111	任意	中継
3	任意	任意	廃棄

(b)

【図 26】

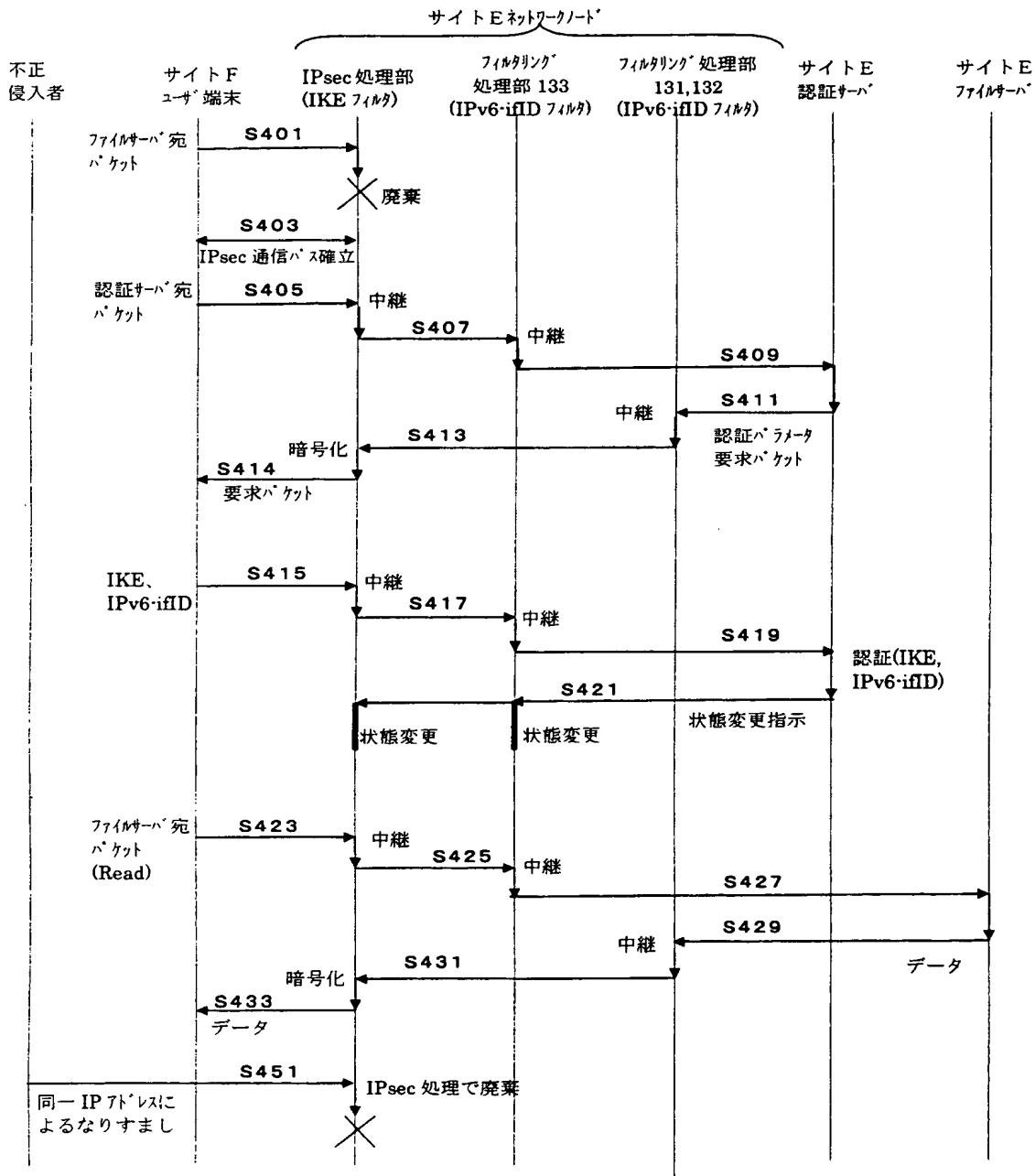
IPv6 インタフェース ID	ネットワークインタフェース部
2222:00FF:FE11:1111	a
2222:00FF:FE22:2222	b
2222:00FF:FEFF:FFFF	y

(a)

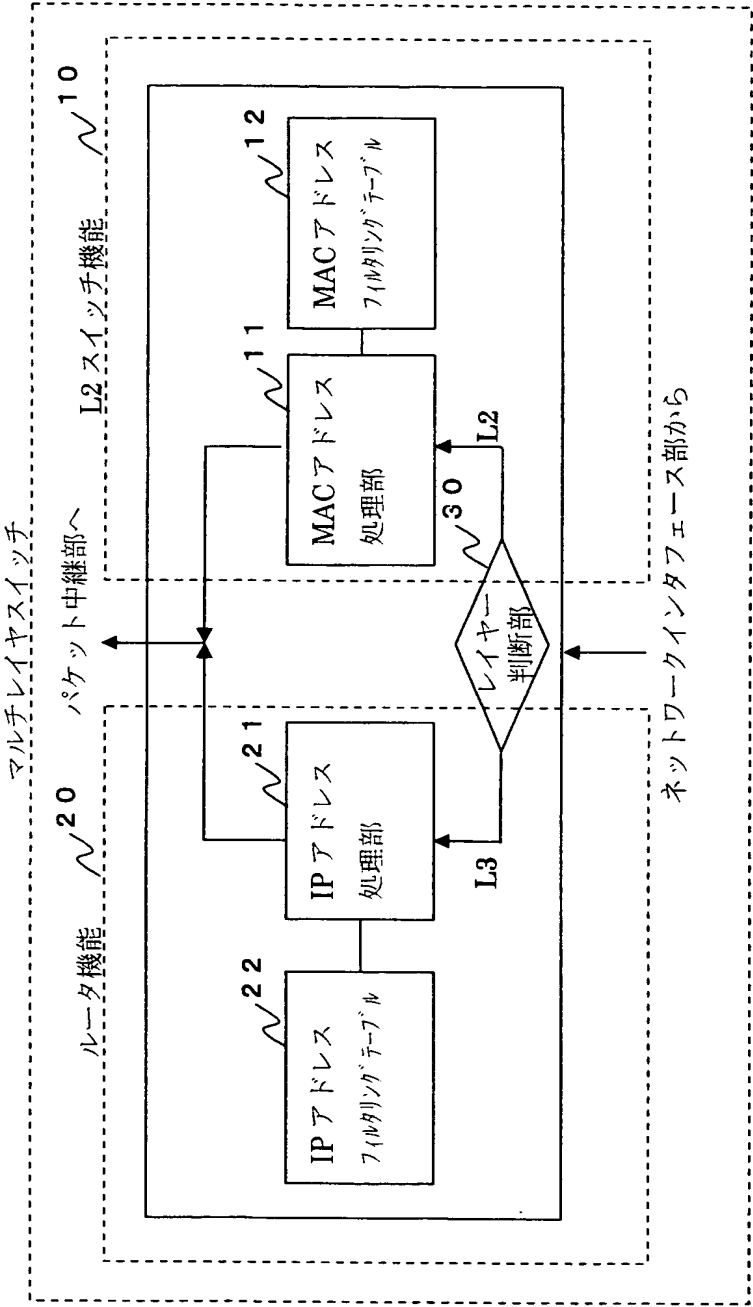
IPv6 インタフェース ID	ネットワークインタフェース部
2222:00FF:FE11:1111	a
2222:00FF:FE22:2222	b
2222:00FF:FEFF:FFFF	y
2222:FFFF:FE00:1	c

(b)

【図 27】



【図 28】



【書類名】 要約書

【要約】

【課題】 アクセスが許可されていない端末、及び、なりすましによる侵入者からのアクセスを拒否するネットワークシステムを提供する。

【解決手段】 認証ノード 1 0 0 のフィルタリング処理部 1 3 1 ～ 1 3 5 は、ネットワークインタフェース部を介して受け取ったパケットが、アクセスを許可された端末からのパケットか、MAC アドレス、IP v 6 アドレスに基づきフィルタリングテーブルを参照して判断し、パケットを中継又は廃棄する。パケット中継部 1 1 0 は、アドレステーブル 1 6 0 を参照し、適宜のネットワークインタフェース部を介してフィルタリング処理部を通過したパケットを宛先アドレスへ中継する。フィルタ変更指示処理部 1 4 0 は、アクセスが許可されたユーザ端末からのパケットを中継させるための状態変更指示を受信し、フィルタリング処理部のフィルタリングテーブルを変更する。

【選択図】 図 2



特願 2 0 0 3 - 0 7 5 8 6 5

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 5 1 0 8 ]

1. 変更年月日

1 9 9 0 年 8 月 3 1 日

[変更理由]

新規登録

住 所

東京都千代田区神田駿河台 4 丁目 6 番地

氏 名

株式会社日立製作所